

AT-S60 Management Software

AT-S60



User's Guide

AT-8400 SERIES SWITCH

VERSION 1.1

PN 613-50400-00 Rev A



Simply connecting the (IP) world

Copyright © 2003 Allied Telesyn, Inc.
960 Stewart Drive Suite B, Sunnyvale, CA 94085 USA

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft is a registered trademark of Microsoft Corporation, Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

List of Figures	9
Preface	12
How This Guide is Organized	12
Document Conventions	13
Where to Find Web-based Guides	14
Contacting Allied Telesyn	15
Online Support.....	15
Email and Telephone Support.....	15
For Sales or Corporate Information	15
Obtaining Management Software Updates	16
Management Software Updates	17

Section I

Overview	18
-----------------------	----

Chapter 1

AT-S60 Overview	19
Overview	20
Local Management Session	21
Telnet Management Session	22
Web Browser Management Session	23
SNMP Management Session	24
Management Access Levels	25
Specifying Ports	26

Section II

Local and Telnet Management	27
--	----

Chapter 2

Starting a Local or Telnet Management Session	28
Local Management Session	29
Starting a Local Management Session.....	30
Enhanced Stacking	32
Quitting from a Local Session	32
Telnet Management Session	33

Starting a Telnet Management Session	33
Quitting from a Telnet Management Interface	34
Chapter 3	
Basic Switch Parameters	35
Assigning an IP Address to a Switch	36
How Do You Assign an IP Address?	37
Configuring an IP Address and Switch Name	38
Configuring Line Cards	41
Displaying the Line Card Information	41
Configuring Line Card Information	42
Activating the BOOTP and DHCP Services	45
Configuring SNMP Community Strings and Trap IP Addresses	47
Enabling SNMP Communities	47
Configuring SNMP Communities	50
Deleting a SNMP Community	52
Modifying a SNMP Community	53
Displaying a SNMP Community	55
Rebooting a Switch	56
Configuring the AT-S60 Software Security Features	57
Configuring the Management Passwords	57
Configuring Management Access	59
Viewing the AT-S60 Hardware and Software Information	60
Displaying System Hardware Information	60
Displaying System Software Information	61
Pinging a Remote System	63
Returning the AT-S60 Software to the Factory Default Values	64
Configuring the Console Startup Mode	66
Chapter 4	
Enhanced Stacking	67
Enhanced Stacking Overview	68
Guidelines	68
Example	70
Setting a Switch's Enhanced Stacking Status	71
Configuring Enhanced Stacking	72
Selecting a Switch in an Enhanced Stack	73
Returning to the Master Switch	75
Chapter 5	
Port Parameters	76
Displaying Port Status	77
Configuring Port Parameters	81
Chapter 6	
Port Security	85
Port Security Overview	86
Automatic	86
Limited	86
Secured	87
Locked	87
Security Violations and Intrusion Actions	87
Configuring Port Security	88

Chapter 7

Port Trunking	92
Port Trunking Overview	93
Port Trunking Guidelines	94
Before Creating Port Trunks	95
Load Distribution Methods	96
Creating a Port Trunk	97
Deleting a Port Trunk	99
Modifying a Port Trunk	100
Changing the Name of the Port Trunk	102
Adding Ports to an Existing Port Trunk	102
Deleting Ports from a Port Trunk	104
Setting Ports in a Trunk	105
Clearing Ports in a Port Trunk	106

Chapter 8

Port Mirroring	107
Port Mirroring Overview	108
Creating a Port Mirror	109
Modifying a Source Port Mirror	111
Deleting a Destination Port Mirror	113
Enabling a Destination Port Mirror	114
Disabling a Destination Port Mirror	115

Chapter 9

STP, RSTP, and MSTP	116
STP and RSTP Overview	117
Bridge Priority and the Root Bridge	118
Mixed STP and RSTP Networks	125
Spanning Tree and VLANs	125
Enabling or Disabling STP, RSTP, or MSTP	128
Configuring STP	130
Configuring STP Bridge Settings	130
Configuring STP Port Settings	132
Displaying STP Port Settings	134
Configuring RSTP	135
Configuring RSTP Bridge Settings	135
Configuring RSTP Port Settings	138
Displaying Port RSTP Status	140
MSTP Overview	141
Multiple Spanning Tree Instance (MTSI)	142
VLAN and MSTI Associations	145
Multiple Spanning Tree Regions	145
Summary of Guidelines	150
Configuring MSTP	156
Configuring MSTP Bridge Settings	156
Configuring the CIST Priority	159
Creating and Deleting MSTI IDs	160
Associating VLANs to MSTI IDs	162
Configuring MSTP Port Settings	165
Displaying MSTP Port Status	166

Chapter 10

Virtual LANs	168
VLAN Overview	169
Port-based VLAN Overview	171
General Rules to Creating a Port-based VLAN	173
Drawbacks to Port-based VLANs	174

Port-based Examples	175
Tagged VLAN Overview	179
General Rules to Creating a Tagged VLAN	181
Tagged VLAN Example	182
Basic VLAN Mode Overview	184
Displaying VLANs	185
Creating a Port-based or Tagged VLAN	187
Example of Creating a Port-based VLAN	191
Example of Creating a Tagged VLAN	192
Modifying a VLAN	193
Deleting a VLAN	196
Setting a Switch's VLAN Mode	197
Specifying a Management VLAN	198

Chapter 11

MAC Address Table	200
MAC Address Overview	201
Displaying MAC Addresses	203
Adding Static MAC Addresses	207
Deleting MAC Addresses	209
Changing the Aging Time	211

Chapter 12

Class of Service	212
Class of Service Overview	213
Configuring CoS	214

Chapter 13

IGMP Snooping	215
IGMP Snooping Overview	216
Activating IGMP Snooping	218
Displaying a List of Host Nodes	220
Displaying a List of Multicast Routers	221

Chapter 14

Ethernet Statistics	222
Displaying Port Statistics	223

Chapter 15

File Downloads and Uploads	225
Overview	226
Obtaining Software Updates	228
Transferring Files from a Local Management Session	229
Transferring Files from a Telnet Session	234
Downloading Files Switch to Switch	237
Uploading Files	239

Section III

Web Browser Management

Chapter 16

Starting a Web Browser Management Session	242
Starting a Web Browser Management Session	243
Browser Tools	245
Quitting from a Web Browser Management Session	245

Chapter 17	
Basic Switch Parameters	246
Configuring an IP Address and Switch Name	247
Activating the BOOTP and DHCP Services	252
Viewing System Information	253
Configuring the SNMP Parameters and Trap IP Addresses	256
Resetting a Switch	262
Pinging a Remote System	263
Returning the AT-S60 Software to the Factory Default Values	264
Chapter 18	
Enhanced Stacking	265
Overview	266
Setting a Switch's Enhanced Stacking Status	266
Selecting a Switch in an Enhanced Stack	267
Chapter 19	
Port Parameters	270
Configuring Port Parameters	271
Displaying Port Status and Statistics	276
Displaying Port Status	276
Displaying Port Statistics	279
Chapter 20	
Port Security	282
Displaying the Port Security Level	283
Chapter 21	
Port Trunks	286
Creating or Deleting a Port Trunk	287
Creating a Port Trunk	287
Deleting a Port Trunk	289
Modifying a Port Trunk	290
Chapter 22	
Port Mirroring	292
Creating or Deleting a Port Mirror	293
Creating a Port Mirror	293
Deleting a Port Mirror	295
Modifying a Port Mirror	295
Chapter 23	
STP, RSTP, and MSTP	297
Activating STP, RSTP, or MSTP	298
Configuring STP	300
Configuring RSTP	304
Configuring MSTP	309
Configuring MSTP and CIST Parameters	309
Associating VLANs to MSTIs	312
Configuring MSTP Port Parameters	315
Displaying STP, RSTP, or MSTP Settings	317

Chapter 24	
Virtual LANs	320
Creating a VLAN	321
Modifying a VLAN	324
Deleting VLANs	326
Displaying VLANs	327
Setting the Switch's VLAN Mode	328
Chapter 25	
MAC Address Table	329
Viewing the MAC Address Table	330
Adding Static and Multicast MAC Addresses	333
Deleting MAC Addresses	335
Changing the Aging Time	336
Chapter 26	
IGMP Snooping	337
Configuring IGMP Snooping	338
Displaying a List of Host Nodes and Multicast Routers	341
Appendix A	
AT-S60 Default Settings	343
Index	346

List of Figures

Figure 1: Connecting a Terminal or PC to the RS-232 Terminal Port	30
Figure 2: Main Menu	31
Figure 3: Administration Menu	38
Figure 4: Line Card Menu	41
Figure 5: Display Line Card Information Menu	42
Figure 6: Configure Line Card Menu	43
Figure 7: Configure Line Card Temperature	43
Figure 8: System Menu	48
Figure 9: Configure System Menu	48
Figure 10: Configure SNMP Menu	49
Figure 11: Configure SNMP Community Menu	50
Figure 12: Modify SNMP Community Menu	53
Figure 13: Display SNMP Community Menu	55
Figure 14: Passwords Menu	58
Figure 15: Display System Hardware Information Menu	60
Figure 16: Display System Fan A Information Menu	61
Figure 17: Display System Software Information Menu	62
Figure 18: Enhanced Stacking Example	70
Figure 19: Enhanced Stacking Menu	72
Figure 20: Stacking Services Menu	73
Figure 21: Updated Stacking Services Menu	74
Figure 22: Port Menu	77
Figure 23: Port Status Menu	78
Figure 24: Port Configuration Menu	81
Figure 25: Port Security Menu	88
Figure 26: Configure Port Security Menu	89
Figure 27: Configure Port Security Menu	89
Figure 28: Port Trunk Example with 1000 Mbps Ports	93
Figure 29: Port Trunk Example with 10/100 Mbps Ports	94
Figure 30: Trunking Configuration Menu	97
Figure 31: Modify Trunk Menu	101
Figure 32: Port Mirroring Menu	109
Figure 33: Point-to-Point Ports	123
Figure 34: Edge Port	124
Figure 35: Point-to-Point and Edge Point	125
Figure 36: VLAN Fragmentation	126
Figure 37: Spanning Tree Menu	128

Figure 38: STP Menu	131
Figure 39: STP Port Parameters Menu	132
Figure 40: Configure STP Port Settings Menu	133
Figure 41: Display STP Port Configuration Window	134
Figure 42: RSTP Menu	136
Figure 43: RSTP Port Parameters Menu	138
Figure 44: Configure RSTP Port Settings Menu	139
Figure 45: VLAN Fragmentation with STP or RSTP	142
Figure 46: MSTP Example of Two Spanning Tree Instances	143
Figure 47: Multiple VLANs in a MSTI	144
Figure 48: Multiple Spanning Tree Region	147
Figure 49: CIST and VLAN Guideline - Example 1	152
Figure 50: CIST and VLAN Guideline - Example 2	152
Figure 51: Spanning Regions - Example 1	154
Figure 52: MSTP Menu	157
Figure 53: CIST Menu	159
Figure 54: MSTI Menu	160
Figure 55: VLAN-MSTI Association Menu	163
Figure 56: MSTP Port Parameters Menu	165
Figure 57: Configure MSTP Port Settings Menu	165
Figure 58: Port-based VLAN - Example 1	175
Figure 59: Port-based VLAN - Example 2	177
Figure 60: Example of a Tagged VLAN	182
Figure 61: VLAN Menu	185
Figure 62: Display VLAN Menu	185
Figure 63: Display VLAN Window	186
Figure 64: Configure VLAN Menu	187
Figure 65: Configure VLAN Menu	188
Figure 66: Modifying VLAN Menu	193
Figure 67: MAC Address Tables Menu	203
Figure 68: Display MAC Addresses Menu	203
Figure 69: Show All MAC Addresses Window	204
Figure 70: Configure MAC Addresses Menu	207
Figure 71: IGMP Snooping Configuration Menu	218
Figure 72: View Multicast Hosts List Window	220
Figure 73: View Multicast Routers List Window	221
Figure 74: Port Statistics Menu	223
Figure 75: Downloads & Uploads Menu	230
Figure 76: Transfer Menu	231
Figure 77: Send File Menu	232
Figure 78: XModem File Send Window	232
Figure 79: Downloads & Uploads Menu	235
Figure 80: Entering a Switch's IP Address in the URL Field	244
Figure 81: Home Page	244
Figure 82: Configuration System Web Page	248
Figure 83: Monitoring Web Page	253
Figure 84: SNMP Web Page	256
Figure 85: Add New SNMP Community Web Page	258
Figure 86: Modify SNMP Community Web Page	260
Figure 87: Ping Client Web Page	263
Figure 88: Factory Default Web Page	264
Figure 89: Enhanced Stacking Web Page	267
Figure 90: Stacking Services Web Page	268
Figure 91: AT-S39 Home Page	269
Figure 92: Port Settings Web Page	271

Figure 93: Configuring Ports Web Page	272
Figure 94: Port Monitoring Web Page	276
Figure 95: Port Status Web Page	277
Figure 96: Port Statistics Web Page	280
Figure 97: Port Security Web Page	283
Figure 98: Security for Ports Web Page	284
Figure 99: Port Trunk Web Page	287
Figure 100: Add New Trunk Web Page	288
Figure 101: Modify Trunk Web Page	291
Figure 102: Port Mirroring Web Page	293
Figure 103: Add New Mirror Web Page	294
Figure 104: Modify Mirror Web Page	296
Figure 105: Spanning Tree Web Page	298
Figure 106: Spanning Tree Expanded Web Page	301
Figure 107: STP Settings Web Page	303
Figure 108: Configure RSTP Parameters	305
Figure 109: RSTP Settings Web Page	307
Figure 110: MSTP Spanning Tree Expanded Web Page	310
Figure 111: Add New MSTI Web Page	313
Figure 112: Modify MSTI Web Page	314
Figure 113: MSTP Port Settings Web Page	315
Figure 114: Monitoring Spanning Tree Web Page	317
Figure 115: Monitor STP Parameters Web Page	318
Figure 116: Monitor STP Settings Web Page	319
Figure 117: VLAN Web Page	321
Figure 118: Add New VLAN Web Page	322
Figure 119: Modify VLAN Web Page	324
Figure 120: Monitoring VLAN Web Page	327
Figure 121: MAC Addresses Web Page	330
Figure 122: MAC Addresses Table Web Page	331
Figure 123: Add Static Unicast MAC Address Web Page	333
Figure 124: Configuration IGMP Web Page	338
Figure 125: Monitoring IGMP Web Page	341

Preface

This guide contains instructions on how to configure an AT-8400 Series Switch using the AT-S60 management software. Within this manual, the AT-8400 Series Switch is often referred to as a switch.

How This Guide is Organized

This manual is divided into three sections.

Section I: Overview

This section contains just one chapter. It reviews the different ways that you can access the AT-S60 management software on a switch. In addition, it describes how to specify ports.

Section II: Local and Telnet Management

The chapters in this section explain how to manage a switch from a local management session or a Telnet management session.

To establish a local management session, you connect a terminal or PC to the RS-232 Terminal Port on the AT-8401 management fabric card which is installed in slot M on the front of the switch.

To establish a Telnet management session, you use the Telnet application protocol. This type of management session can be performed from any workstation on your network.

Section III: Web Browser Management

The chapters in this section explain how to manage a switch using a web browser, such as Microsoft® Internet Explorer or Netscape® Navigator, from a workstation on your network.

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.



Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.



Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in Portable Document Format (PDF) from on our web site at www.alliedtelesyn.com. You can view the documents on-line or download them onto a local workstation or server.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base from the following web site: **kb.alliedtelesyn.com**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: **www.alliedtelesyn.com**.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select **Contact Us** then **Worldwide Contacts**.

Obtaining Management Software Updates

New releases of management software for our managed products can be downloaded from either of the following Internet sites:

- the Allied Telesyn web site: **<http://www.alliedtelesyn.com>**
- the Allied Telesyn FTP server: **<ftp://ftp.alliedtelesyn.com>**

If you would prefer to download new software from the Allied Telesyn FTP server from your workstation's command prompt, you will need FTP client software and you will be asked to log in to the server. Enter 'anonymous' as the user name and your email address for the password.

Management Software Updates

New releases of management software for our managed products are available from our web site at www.alliedtelesyn.com and our FTP server at [ftp.alliedtelesyn.com](ftp://ftp.alliedtelesyn.com). To use the FTP server, enter 'anonymous' for the user name when you log in and your e-mail address for the password.

Section I

Overview

The chapter in Section I provides a brief overview of the AT-S60 management software. It explains the functions that you can perform with the management software and reviews the different methods for accessing the AT-S60 software on an AT-8400 switch.

Chapter 1

AT-S60 Overview

This chapter describes the AT-S60 software functions, the types of sessions you can use to access the software, and the management access levels. This chapter contains the following sections:

- ❑ **Overview** on page 20
- ❑ **Local Management Session** on page 21
- ❑ **Telnet Management Session** on page 22
- ❑ **Web Browser Management Session** on page 23
- ❑ **SNMP Management Session** on page 24
- ❑ **Management Access Levels** on page 25
- ❑ **Specifying Ports** on page 26

Overview

The AT-S60 management software is intended for the AT-8400 Series switch. The software is used to monitor and adjust a switch's operating parameters. Functions that you can perform with the software include:

- ☐ Enable and disable ports
- ☐ Configure port parameters, such as port speed and duplex mode
- ☐ Create virtual LANs (VLANs)
- ☐ Create port trunks and port mirrors
- ☐ Assign an Internet Protocol (IP) address and subnet mask
- ☐ Activate and configure the Spanning Tree Protocol (STP)
- ☐ Configure port security

The AT-S60 management software comes pre-installed on the AT-8401 management card with default settings for all operating parameters. If the default settings are adequate for your network, you can use the switch as an unmanaged switch simply by connecting the unit to your network, as explained in the hardware installation guide, and powering on the device.

Note

The default settings for the management software can be found in **Appendix A, AT-S60 Default Settings** on page 343.

To actively manage a switch, such as to change or adjust the operating parameters, you must access the switch's AT-S60 management software. The AT-S60 software has a menu interface that makes it very easy to use and a web interface for managing a switch with a web browser. In addition, you can use a command line interface to manage the switch, as explained in the **AT-S60 Management Software Command Line Interface User's Guide (PN 613-50401-00)**.

There are four different ways that you can access the management software on an AT-8400 switch. The methods are referred to as management sessions in this guide. They are:

- ☐ Local Management Session
- ☐ Telnet Management Session
- ☐ Web Browser Management Session
- ☐ SNMP Management Session

The following sections in this chapter briefly describe each type of management session. In addition, an explanation of how to specify ports is provided.

Local Management Session

You establish a local management session with an AT-8400 switch by connecting a terminal or a PC with a terminal emulator program to the RS-232 Terminal port on the AT-8401 management card, using a straight-through RS-232 cable. This type of management session is referred to as local because you must be physically close to the switch, such as in the wiring closet where the switch is located.

Once the session is started, you will see a menu from which you can make selections to configure and monitor the switch. You can configure all of a switch's operating parameters from a local management session.

Note

For instructions on starting a local management session, refer to **Starting a Local Management Session** on page 30.

Telnet Management Session

Any management workstation on your network that has the Telnet application protocol can be used to manage an AT-8400 switch. This type of management session is referred to in this guide as a remote management session because you do not have to be in the same wiring closet as the switch you are managing. Instead, you can manage the switch from any workstation on the network that has the application protocol.

To establish a Telnet management session with a switch, there must be at least one AT-8400 switch, or an AT-8000 Series switch, on the subnet that has been assigned an Internet Protocol (IP) address. Only one switch in a subnet needs to have an IP address. Once you have established a Telnet management session with the switch that has an IP address, you can use the enhanced stacking feature of the AT-S60 software to access all AT-8400 switch and AT-8000 Series switches in the same subnet.

Note

For further information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 68.

Note

For instructions on how to start a Telnet management session, refer to **Starting a Telnet Management Session** on page 33.

A Telnet management session gives you complete access to all of a switch's operating parameters. You can perform nearly all the same functions from a Telnet management session as you can from a local management session.

Web Browser Management Session

You can also use a web browser to manage a switch. Using a web browser management session is also referred to as remote management, just like a Telnet management session. You can manage a switch from any workstation on your network that has a web browser.

Note

For instructions on starting this type of management session, refer to **Starting a Web Browser Management Session** on page 243.

SNMP Management Session

Another way to remotely manage the switch is with an SNMP management program. A familiarity with Management Information Base (MIB) objects is necessary for this type of management.

The AT-S60 software supports the following MIBs:

- ☐ SNMP MIB-II (RFC 1213)
- ☐ Bridge MIB (RFC 1493)
- ☐ Interface Group MIB (RFC 2863)
- ☐ Ethernet MIB (RFC 1643)
- ☐ Remote Network MIB (RFC 1757)

You must download the Allied Telesyn managed switch MIB file from the Allied Telesyn web site and compile the file with your SNMP program. For instructions, refer to your SNMP management documentation.

For information about how to configure SNMP communities using a local or Telnet management session, see **Configuring SNMP Community Strings and Trap IP Addresses** on page 47.

Note

SNMP management does not utilize the enhanced stacking feature. Consequently, you must assign an IP address to each switch to be managed with an SNMP program.

Management Access Levels

There are two levels of management access on an AT-8400 switch: Manager and Operator. When you log in as a Manager, you can view and configure all of a switch's operating parameters. When you log in as an Operator, you can only view the operating parameters. As an Operator, you cannot change any values.

To log in, you enter a login id of Manager or Operator and the appropriate password when you start an AT-S60 management session. For Manager access, enter the following at the prompts:

```
Login: manager  
password: friend
```

For Operator access, enter the following at the prompts:

```
Login: operator  
password: operator
```

The password is case-sensitive for both Manager and Operator access.

There are a total of 14 login sessions available using the console, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The console and Telnet sessions allow a total of 10 active sessions. While a web browser management session, allows four active login sessions.

Specifying Ports

Many of the commands and parameters, in this manual involve specifying the port(s) on the switch. Port numbers are specified in the following format:

`slot.port`

Slot is the number of the slot in the switch that contains the line card with the port. There are twelve line card slots in the AT-8400 chassis. Port is the port number on the line card. For example, to indicate port 4 on the line card in Slot 8, you would use:

`8.4`

In many commands, you can specify a list of ports. You can list ports on the same line card individually, as a range, or both. The following example refers to Ports 1, 3, and 5 to 8 on the line card in Slot 3:

`3.1,3,5-8`

Some commands can be performed on ports on different line cards. This example refers to Ports 1 and 4 on the line card in Slot 4 and Ports 6 through 8 on the line card in Slot 11:

`4.1,4,11.6-8`

Section II

Local and Telnet Management

The chapters in Section II explain how to manage an AT-8400 switch from a local or Telnet management session. The chapters include:

- ☐ **Chapter 2: Starting a Local or Telnet Management Session** on page 28
- ☐ **Chapter 3: Basic Switch Parameters** on page 35
- ☐ **Chapter 4: Enhanced Stacking** on page 67
- ☐ **Chapter 5: Port Parameters** on page 76
- ☐ **Chapter 6: Port Security** on page 85
- ☐ **Chapter 7: Port Trunking** on page 92
- ☐ **Chapter 8: Port Mirroring** on page 107
- ☐ **Chapter 9: STP, RSTP, and MSTP** on page 116
- ☐ **Chapter 10: Virtual LANs** on page 168
- ☐ **Chapter 11: MAC Address Table** on page 200
- ☐ **Chapter 12: Class of Service** on page 212
- ☐ **Chapter 13: IGMP Snooping** on page 215
- ☐ **Chapter 14: Ethernet Statistics** on page 222
- ☐ **Chapter 15: File Downloads and Uploads** on page 225

Chapter 2

Starting a Local or Telnet Management Session

This chapter contains the procedure for starting a local or Telnet management session on an AT-8400 Series switch. It contains the following sections:

- ❑ **Local Management Session** on page 29
- ❑ **Telnet Management Session** on page 33

Local Management Session

To establish a local management session using the AT-S60 management software, connect an RS-232 straight-through cable to the RS-232 terminal port on the AT-8400 chassis. Connect the other end of the cable to a terminal or a PC with a terminal emulator program.

A local management session is so named because you must be physically close to the switch, usually within a few meters, to start this type of management session. A local management session requires you to connect a terminal directly to the switch. Typically, this means that you are in the wiring closet where the switch is located.

A switch does not need an IP address to be managed from a local management session. You can start a local management session at any time on any AT-8400 switch in your network. Running a local management session does not interfere with the flow of Ethernet traffic through the unit.

Starting a local management session on a switch that has been configured as a Master switch of an enhanced stack allows you to manage all the switches in the subnet from the same local management session. You do not have to start a separate local management session for each switch. This can simplify network management.

There are a total of 14 login sessions available using the console, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The console and Telnet sessions allow a total of 10 active sessions. While a web browser management session, allows four active login sessions.

Note

For information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 68.

Starting a Local Management Session

To start a local management session, perform the following procedure:

1. Connect one end of a straight-through RS-232 cable with a DB-9 connector to the RS-232 terminal port on the AT-8401 management card which is installed in slot M of the chassis.

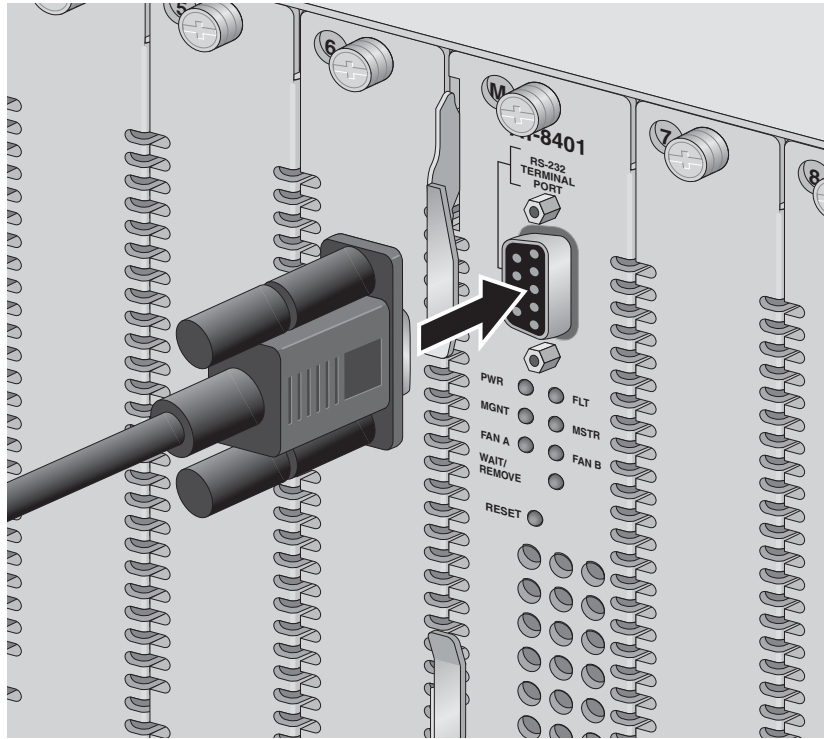


Figure 1 Connecting a Terminal or PC to the RS-232 Terminal Port

2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
 - ☐ Baud rate: 9600 bps (default)
 - ☐ Data bits: 8
 - ☐ Parity: None
 - ☐ Stop bits: 1
 - ☐ Flow control: None

Note

The port settings provided are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

4. Press the Return key twice.

5. You are prompted to input a login id and password.

When prompted for the user name and password, enter one of the following options.

- ☐ For Manager access, type **manager** as the login id. The default password is "friend". Then press Return.
- ☐ For Operator access, type **operator** as the login id. The default password is "operator". Then press Return.

Note

The user names cannot be changed. The passwords are case sensitive. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 57. For information on the two access levels, refer to **Management Access Levels** on page 25.

The Main Menu is displayed in Figure 2.

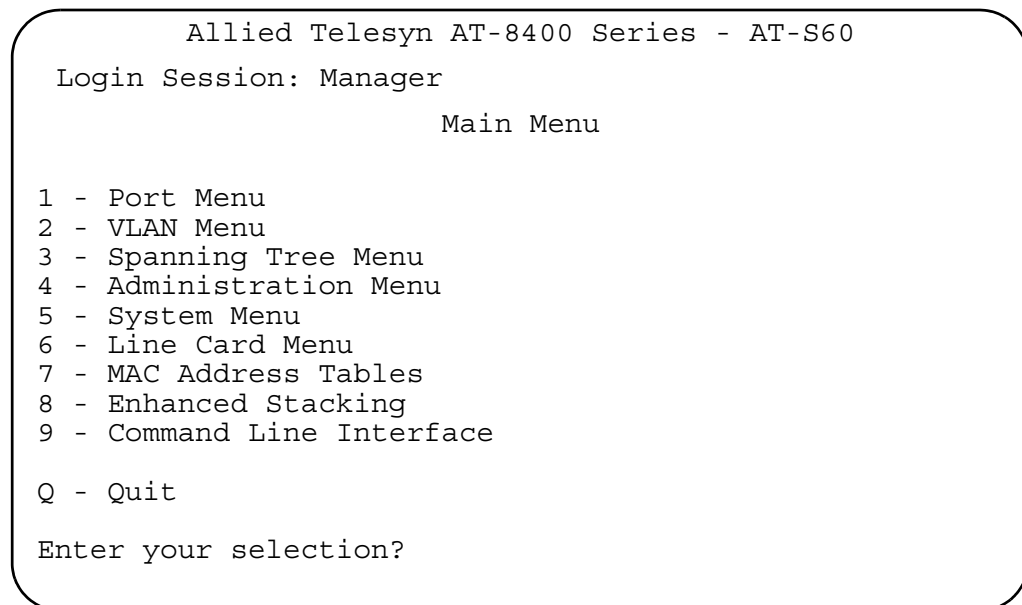


Figure 2 Main Menu

To select a menu item, type the corresponding letter or number.

Pressing the Esc key or typing the letter **R** in a submenu or window returns you to the previous menu.

Please note the following:

- ❑ The Command Line Interface selection in the Main Menu is not described in this manual. For instructions on this option, refer to the **AT-S60 Management Software Command Line Interface User's Guide (PN 613-50401-00)**.
- ❑ If a pound sign (#) or dollar sign (\$) is displayed instead of the Main Menu, the console interface has been configured for a command line prompt when a management session is started. The pound sign means that you logged in as the Manager and the dollar sign means you logged in as an Operator. To display the Main Menu, type **menu** and press Return.
- ❑ During boot up, the switch displays the following message:
Press any key to stop image loading and go to Boot Prompt. This message is for manufacturing purposes only. If you do inadvertently display the boot prompt (=>), type **boot** and press Return to start the switch's software.

Enhanced Stacking

When you start a management session on an AT-8400 or AT-8000 Series switch that has been designated as the Master switch of an enhanced stack, you can manage all the switches in the same subnet from the same management session. This can save you time because you do not have to start a separate local management session each time you want to manage a switch in your network. It can also save you from having to go to the different wiring closets where the switches are located.

For information on enhanced stacking and how to manage different switches from the same management session, refer to **Chapter 4, Enhanced Stacking** on page 67.

Quitting from a Local Session

To quit a local session, return to the Main Menu and type **Q** for Quit.

Allied Telesyn recommends that you exit from a management session when you are finished managing a switch. This can prevent unauthorized individuals from making changes to a switch's configuration should you leave your management station unattended.

Note

The AT-S60 management software automatically ends a management session if it does not detect any activity from the local management station after the specified period of time. The default for the console timeout value is 10 minutes. To change this console value setting, refer to **Configuring Management Access** on page 59.

Telnet Management Session

You can use the Telnet application protocol from a workstation on your network to manage an AT-8400 switch. This type of management is referred to as remote management because you can be physically far from the switch when you start the session. (In contrast to a local management session, which requires that you connect a terminal directly to the switch.) Any workstation on your network that has the application protocol can be used to manage the switch.

In terms of functionality, except for the security features, there are almost no differences between managing a switch locally through the RS-232 Terminal Port and remotely with the Telnet application protocol. You see the same menu selections and have nearly the same management capabilities.

Starting a Telnet management session requires that there be at least one AT-8400 or an AT-8000 Series switch on your network that has an IP address. The switch with the IP address is referred to as the master switch. Once you have started a Telnet management session on the master switch, you have management access to all the other AT-8400 and AT-8000 Series switches that reside in the same subnet.

There are a total of 14 login sessions available using the console, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The console and Telnet sessions allow a total of 10 active sessions. While a web browser management session, allows four active login sessions.

Note

For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 68.

Starting a Telnet Management Session

To start a Telnet management interface, specify the IP address of the Master switch of the stack in the Telnet application protocol.

When prompted for the user name and password, enter one of the following options.

- ☐ For Manager access, type **manager** as the user name. The default password is "friend".
- ☐ For Operator access, type **operator** as the user name. The default password is "operator".

Note

The user names cannot be changed. The passwords are case sensitive. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 57. For information on the two access levels, refer to **Management Access Levels** on page 25.

The Main Menu of a Telnet management interface is the same menu that you see in a local management interface, shown in Figure 2 on page 31. Nearly all the functions from a local management interface are available to you from a Telnet management interface.

The menus also function in the same manner. To make a selection, type its corresponding number or letter. To return to a previous menu, type **R** or press the Esc key.

Quitting from a Telnet Management Interface

To end a Telnet management interface, return to the Main Menu and type **Q** for Quit.

Note

The AT-S60 management software automatically ends a management session if it does not detect any activity from the remote management station after the specified period of time. The default for the console timeout value is 10 minutes. To change this console value setting, refer to **Configuring Management Access** on page 59.

Chapter 3

Basic Switch Parameters

This chapter contains a variety of information about basic switch parameters and procedures for using them with a local or Telnet management session. There is a discussion on when to assign an IP address to a switch. There are also procedures for resetting the switch, activating the original switch default settings, and more.

This chapter contains the following sections:

- ☐ **Assigning an IP Address to a Switch** on page 36
- ☐ **Configuring an IP Address and Switch Name** on page 38
- ☐ **Configuring Line Cards** on page 41
- ☐ **Activating the BOOTP and DHCP Services** on page 45
- ☐ **Configuring SNMP Community Strings and Trap IP Addresses** on page 47
- ☐ **Rebooting a Switch** on page 56
- ☐ **Configuring the AT-S60 Software Security Features** on page 57
- ☐ **Viewing the AT-S60 Hardware and Software Information** on page 60
- ☐ **Pinging a Remote System** on page 63
- ☐ **Returning the AT-S60 Software to the Factory Default Values** on page 64
- ☐ **Configuring the Console Startup Mode** on page 66

Assigning an IP Address to a Switch

When building or expanding your network, you need to decide which managed switches need an unique IP addresses. The rule used to be that a managed switch needed a IP address if you wanted to manage it remotely, such as with the Telnet application protocol. However, if a network contained a lot of managed switches, having to assign each one an IP address was often cumbersome and time consuming. Also, it was often difficult keeping track of all the IP addresses.

The enhanced stacking feature of the AT-8400 switch simplifies when to assign an IP address. With enhanced stacking, you need assign an IP address to only one AT-8400 or AT-8000 Series switch, in each subnet in your network. The switch with the IP address is referred to as the Master switch of the subnetwork. All switches in the same subnet share the IP address.

Starting a local or remote management session on the Master switch automatically gives you complete management access to all the other switches in the same subnet.

This feature has two primary benefits. First, it helps reduce the number of IP addresses you have to assign to your network devices. Second, it allows you to configure multiple switches through the same local or remote management session.

If your network consists of multiple subnets, you must assign a unique IP address to at least one switch in each subnet. The switch with the IP address will be the Master switch of that subnet.

When you assign a switch an IP address, you must also assign it a subnet mask. The switch uses the subnet mask to determine which portion of an IP address represents the network address and which the node address.

You must also assign the switch a gateway address if there is a router between the switch and the remote management workstation. This gateway address is the IP address of the router through which the switch and management station will communicate.

Note

For further information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 68.

If you do not plan to remotely manage any of the AT-8400 switch in your network, then you do not need to assign an IP address to any of them. The switches will operate fine without an IP address and you will still be able to manage them completely using local management sessions.

How Do You Assign an IP Address?

Once you have decided which, if any, switches on your network need an IP address, you have to access the AT-S60 software on the switches and assign the address or addresses. There are actually two ways in which a switch can obtain an IP address.

The first method is to assign the IP configuration information manually which is explained in the next procedure. Initially assigning an IP address to a switch can only be done through a local management session.

The second method is to activate the BOOTP and DHCP services on the switch and have the switch automatically download its IP configuration information from a BOOTP or DHCP server on your network. This procedure is explained in **Activating the BOOTP and DHCP Services** on page 45.

Configuring an IP Address and Switch Name

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to the switch using a local or Telnet management session. (If you want the switch to obtain its IP configuration from a DHCP or BOOTP server on your network, go to the procedure **Activating the BOOTP and DHCP Services** on page 45.)

In addition, this procedure explains how to assign a name to the switch, along with other optional information, such as the name of the administrator responsible for maintaining the unit and the location of the switch.

To manually set a switch's IP address, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.

The Administration Menu is displayed in Figure 3.

```
Allied Telesyn AT-8400 Series - AT-S60
Login Privilege: Manager
Administration Menu

1 - IP Address ..... 0.0.0.0
2 - Subnet Mask ..... 0.0.0.0
3 - Default Gateway ..... 0.0.0.0
4 - System Name .....
5 - Administrator .....
6 - Comments .....
7 - Set Password .....
8 - BOOTP/DHCP ..... Disabled
9 - Set Console Baud Rate .... 9600 bps

B - Reboot the switch
D - Downloads & Uploads
P - Ping a remote system

R - Return to Previous Menu

Enter your selection?
```

Figure 3 Administration Menu

2. Change the parameters as desired.

The parameters in the Administrative Menu are described below:

1 - IP Address

This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program, or if you want a switch to function as the Master switch of an enhanced stack.

2 - Subnet Mask

This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch.

3 - Default Gateway

This parameter specifies the default router's IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router.

4 - System Name

This parameter specifies a name for the switch (for example, Sales Ethernet switch). This parameter is optional.

Note

Allied Telesyn recommends that you assign each switch a name because they help you identify the various switches when you manage them. In addition, switch names help you avoid performing a configuration procedure on the wrong switch.

5 - Administrator

This parameter specifies the name of the network administrator responsible for managing the switch. This parameter is optional.

6 - Comments

This parameter specifies additional information about the Fast Ethernet switch, such as its location (for example, 4th Floor - wiring closet 402B). This parameter is optional.

7 - Set Password

This parameter is used to change the Manager and Operator's login passwords. For instructions, refer to **Configuring the Management Passwords** on page 57.

8 - BOOTP/DHCP

This selection activates and deactivates the BOOTP and DHCP services on the switch. For information on this selection, refer to **Activating the BOOTP and DHCP Services** on page 45.

9 - Set Console Baud Rate

This selection allows you set the baud rate of the serial port on the AT-8401 management card. The range is 2400 to 115,200 bps. This menu selection is only available from a local management session. The default is 9600 bps.

B - Reboot the switch

This selection allows you to reboot the switch.

D - Downloads & Uploads

For information on this selection, refer to **Chapter 15, File Downloads and Uploads** on page 225.

R - Ping a Remote System

For information on this selection, refer to **Pinging a Remote System** on page 63.

3. After you have set the parameters, type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

Note

Changes to any of the parameters on this menu, including the IP address, subnet mask, or gateway address, are immediately activated on a switch.

Configuring Line Cards

This section describes how to manually configure line cards for the AT-8400 switch. The following procedures are provided:

- ☐ Displaying the Line Card Information
- ☐ Configuring the Line Card Information

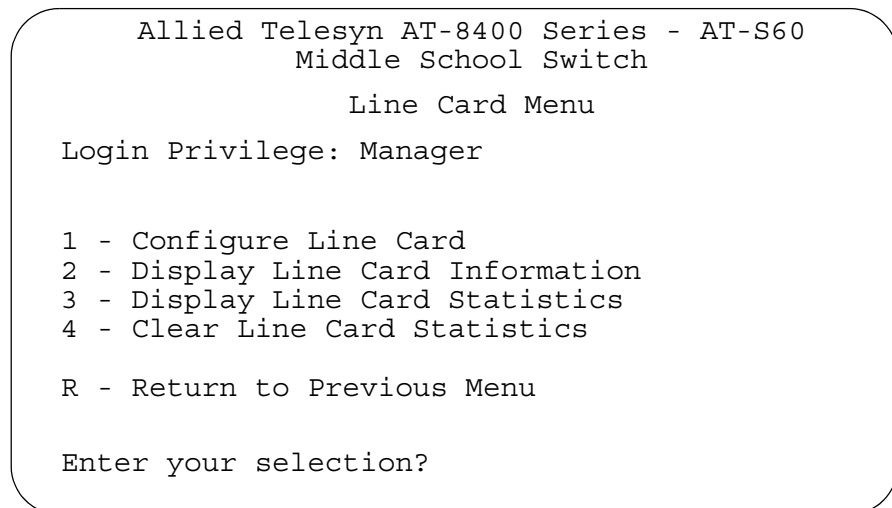
Displaying the Line Card Information

Use this procedure to display the line cards and the AT-8401 management card, installed in your AT-8400 chassis. Naturally, this procedure is very useful if your chassis is in a remote location and you need to know what cards are installed in the chassis.

To display the current line card configuration, perform the following procedure:

1. From the Main Menu, type **6** to select the Line Cards Menu.

The Line Card Menu is displayed in Figure 4.



```
Allied Telesyn AT-8400 Series - AT-S60
Middle School Switch

Line Card Menu

Login Privilege: Manager

1 - Configure Line Card
2 - Display Line Card Information
3 - Display Line Card Statistics
4 - Clear Line Card Statistics

R - Return to Previous Menu

Enter your selection?
```

Figure 4 Line Card Menu

2. Select **2** - Display Line Card to display the current line cards installed your AT-8400 chassis.

The Display Line Card Information Menu is displayed in Figure 5.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Middle School Switch

Login Privilege: Manager

Display Line Card Information

Line Card      Serial Number      Model Name Temperature Upper/Lower Threshold
              (C Degree) (C Degree)
=====
SCP           A00501S03040001G      AT-8401      26              80/75
1             S05525A023600007      AT-8411      25              80/-25
2             S05525A023600001      AT-8411      25              80/-25
3             S05525A023600102      AT-8411      25              80/-25
7             S05525A023600019      AT-8413      25              80/-25
8             S05525A023600001      AT-8413      25              80/-25
9             S05525A023600201      AT-8413      25              80/-25

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 5 Display Line Card Information Menu

The SCP entry represents the AT-8401 management card which is installed in slot M of the chassis.

3. Select **U** - Update the Display to update the display after you have installed or removed line cards from your chassis.

Configuring Line Card Information

Use the configuring line card information procedure to configure the temperature ranges for AT-8401 management card and the line cards. The temperatures given are in centigrade.

You may want to alter the temperature ranges if your chassis is located in a very warm or cold climate. If the line cards or the AT-8401 management card reach the lower threshold of the range, a trap message is sent to the network administrator. If the line cards or the AT-8401 management card reach the upper threshold of the temperature range, a trap is sent to the management software.

To change the temperature requirements for the line cards and the AT-8401 management card, perform the following procedure.

1. From the Main Menu, type **6** to select Line Card Menu.
The Line Card Menu is displayed in Figure 4 on page 41.
2. Select **1** - Configure Line Card.

The Configure Line Card Menu is displayed in Figure 6.

```

Allied Telesyn AT-8400 Series - AT-S60
Middle School Switch
Login Privilege: Manager
Configure Line Card

1 - Configure Line Card Temperature
R - Return to Previous Menu
Enter your selection?

```

Figure 6 Configure Line Card Menu

3. Select **1** - Configure Line Card Temperature to change the acceptable temperature range for a line card. The temperatures provided are in centigrade. You may want to alter the temperature ranges if the chassis is located in a cold or warm climate.

The Configure Line Card Temperature Menu appears as shown in Figure 7.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
High School Switch
Login Privilege: Manager
Configure Line Card Temperature
Line Card    Current Temperature  Upper Threshold  Lower Threshold
              (C Degree)        (C Degree)        (C Degree)
=====
SCP           27                80                75
04            26                80               -25
08            26                80               -25

1 - Set Upper Temperature Threshold
2 - Set Lower Temperature Threshold
R - Return to Previous Menu
Enter your selection?

```

Figure 7 Configure Line Card Temperature

4. Select **1** - Set Upper Temperature Threshold to set the upper temperature range of a line card.

The following prompt appears:

```
Enter the line card number (0-12), 0 is SCP card ->  
[0 to 12] -> 0
```

5. Enter the slot number of the line card to change its upper temperature threshold. Or, enter 0 to change the temperature range of the AT-8401 management card. Then press Return.

Once you enter the slot number, the following prompt appears:

```
Enter the Temperature Threshold -> [-55 to 125] -> 0
```

6. Enter a value from -55 to 125 to indicate the upper temperature threshold in centigrade. Then press Return.

Once you enter a value here, the Configure Line Card Temperature Menu is updated with the new values.

7. Select **2** - Set Lower Temperature Threshold to change the lower temperature threshold of a line card.

The following prompt appears:

```
Enter the line card number (0 - 12), 0 is SCP card  
-> [0 to 12] -> 0
```

8. Enter the slot number of the line card to change its lower temperature threshold. Enter 0 to indicate the AT-8401 management card which resides in slot M. Enter 1 through 12 to indicate the cards in slots 1 through 12 of the chassis. Then press Return.

After you enter a line card number, the following prompt appears:

```
Enter Temperature Threshold -> [-55 to 125] -> 0
```

9. Enter a lower temperature threshold between -55 and 125 degrees centigrade. Then press Return.

The Configure Line Card Temperature Menu is updated with the new value.

10. Type **R** until you return to the Main Menu. Then type **S** to select Save Configuration changes.

Activating the BOOTP and DHCP Services

The BOOTP and DHCP application protocols were developed to simplify network management. They are used to automatically assign IP configuration information--such as an IP address, subnet mask, and a default gateway address--to the devices on your network.

An AT-8400 switch supports these protocols and can obtain its IP configuration information from a BOOTP or DHCP server on your network. If you activate this feature, the switch seeks its IP address and other IP configuration information from a BOOTP or DHCP server on your network whenever you reset or power cycle the device.

Naturally, for this to work there must be a BOOTP or DHCP server residing on your network and you must configure the service by entering in the switch's MAC address.

BOOTP and DHCP services typically allow you to specify how the IP address is assigned to the switch. The choices are static and dynamic. If you choose static, the server always assigns the same IP address to the switch when the switch is reset or powered ON. This is the preferred configuration. Since the BOOTP and DHCP services always assigns the same IP address to a switch, you will know which IP address to use when you need to remotely manage a particular switch.

If you specify the IP address as dynamic, the server assigns the switch any unused IP address. As a result, a switch might have a different IP address each time you reset or power cycle the device, making it difficult for you to remotely manage the unit.

Note

The BOOTP and DHCP option is disabled by default on the switch.

To activate or deactivate the BOOTP and DHCP protocols on the switch, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.

The Administration in Figure 3 on page 38 is displayed.

2. Type **8** to select BOOTP/DHCP.

The following prompt is displayed:

BOOTP/DHCP (E-Enabled, D-Disabled):

3. Type **E** to enable BOOTP and DHCP services on the switch or **D** to disable the services. Then press Return. The default is disabled.

Note

If you activate BOOTP/DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

4. Type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring SNMP Community Strings and Trap IP Addresses

The procedures in this section allow you to create and modify SNMP communities that have access to the switch. When you create an SNMP community, you can specify SNMP management station IP addresses as well as trap receiver IP addresses. The following procedures are provided:

- ❑ **Enabling SNMP Communities** on page 47
- ❑ **Configuring SNMP Communities** on page 50
- ❑ **Deleting a SNMP Community** on page 52
- ❑ **Modifying a SNMP Community** on page 53
- ❑ **Displaying a SNMP Community** on page 55

Enabling SNMP Communities

To configure SNMP, you need to enable SNMP on your switch. Then you can enable authentication failure traps. However, this is an optional step.

Traps generated by the SNMP agent are forwarded to all trap receivers in all of the SNMP communities. (For information about configuring the trap host receiver IP addresses and the SNMP management stations, see **Configuring SNMP Communities** on page 50.) The SNMP community name and manager IP addresses are used to provide authentication. An incoming SNMP message is deemed authentic if it contains a valid community name and it originated from an IP address that is defined as a management station for that community.

When a community is disabled, the SNMP agent behaves as if the community does not exist, and the switch generates authentication failure traps for messages directed to the disabled community.

SNMP authentication is a mechanism where an SNMP message is declared to be authentic. The authentication failure trap may be generated as a result of the failure to authenticate an SNMP message. See the procedure below for instructions on how to enable or disable the generation of authentication failure traps.

To enable SNMP and authentication trap messages, perform the following procedure.

1. From the Main Menu, type **5** to select System Menu.

The System Menu in Figure 8 is displayed.

```
Allied Telesyn AT-8400 Series - AT-S60
Administration Building Switch

Login Privilege: Manager

                        System Menu

1 - Configure System
2 - Display System Hardware Information
3 - Display System Software Information
4 - Display System Statistics
5 - Clear System Statistics

R - Return to Previous Menu
```

Figure 8 System Menu

2. From the System Menu, type **1** to select Configure System.

The Configure System Menu is displayed in Figure 9.

```
Allied Telesyn AT-8400 Series - AT-S60
Administration Building Switch

Login Privilege: Manager

                        Configure System

1 - Switch Mode ..... Tagged
2 - Console Disconnect Timer Interval ..... 10 minute(s)
3 - Web Server Status ..... Enabled
4 - MAC address aging time ..... 300 second(s)
5 - Console Startup Mode ..... Menu
6 - Configure IGMP Snooping
7 - Configure SNMP

D - Reset to Factory Defaults
R - Return to Previous Menu

Enter your selection?
```

Figure 9 Configure System Menu

- From the Configure System window, type **7** to select Configure SNMP. The Configure SNMP Menu is displayed in Figure 10.

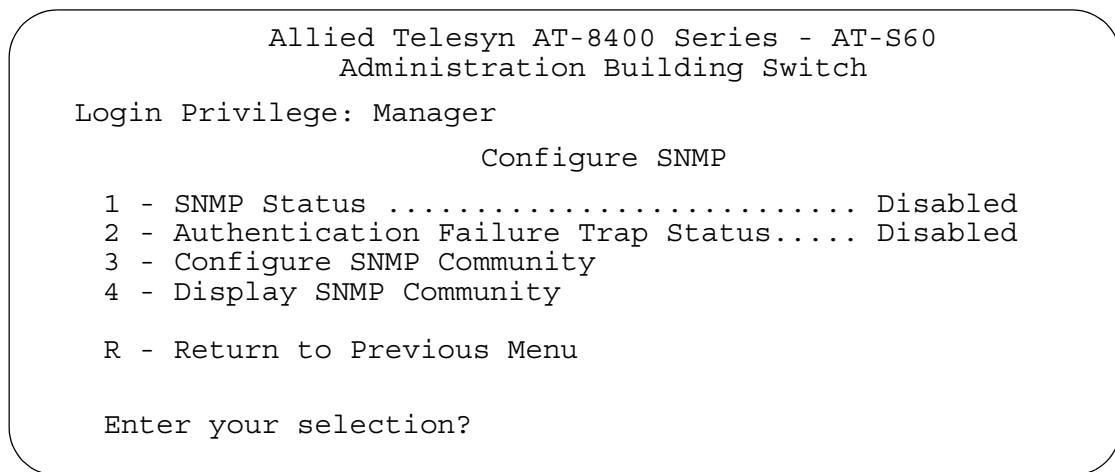


Figure 10 Configure SNMP Menu

- Select **1** - SNMP Status to enable or disable SNMP management on your switch.
Toggle between Enabled and Disabled by pressing **1** again.
- Select **2** - Authentication Failure Trap Status to configure the switch to send an authentication failure trap to trap receiver hosts. When this parameter is enabled, the switch sends an authentication failure trap under two conditions:

- The SNMP management station attempts to access the switch using an incorrect or invalid community name
- The IP address of this SNMP management station is not configured as an SNMP manager within the community.

Toggle between Enabled and Disabled by pressing **2** again. If you do not configure a trap receiver IP address, no trap message is sent.

Enabled - Sends authentication failure traps to IP addresses of configured trap receiver hosts.

Disabled - Does not send authentication failure traps.

- After making your changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Changes to the SNMP parameters are immediately activated on the switch.

Configuring SNMP Communities

Use this procedure to configure the SNMP community strings for the switch. You can assign SNMP community names. In addition, you can assign up to eight IP addresses of management stations and up to eight IP addresses of trap receivers. In addition, the following procedure permits you to modify current SNMP community parameters as well as delete SNMP community access.

Use the following procedure to configure SNMP.

1. From the Main Menu, type **5** to select System Menu.
The System Menu in Figure 8 on page 48 is displayed.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is displayed in Figure 9 on page 48.
3. From the Configure System window, type **7** to select Configure SNMP.
The Configure SNMP Menu is displayed in Figure 10 on page 49.
4. Select **3** - Configure SNMP Community to configure SNMP parameters.

The Configure SNMP Community menu appears:

```

Allied Telesyn AT-8400 Series - AT-S60
Administration Building Switch

Login Privilege: Manager

                                Configure SNMP Community

Community Name  Access Mode  Status  Manager IP Address  Trap Receiver IP
=====
private         Read|Write  Enabled  ALL IP
public          Read Only  Enabled  ALL IP

1 - Create SNMP Community
2 - Delete SNMP Community
3 - Modify SNMP Community

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 11 Configure SNMP Community Menu

5. Select **1** - Create SNMP Community to configure SNMP parameters.
The following prompt appears:

Enter SNMP Community Name:

6. Enter a SNMP community name of up to 15 alphanumeric characters and press Return. This parameter is case sensitive.

Note

Community names act as passwords for the SNMP protocol. Allied Telesyn recommends that you select SNMP community names carefully to ensure these names are known only to authorized personnel.

The following prompt appears:

Enter Access Mode [R-Read Only, W-Read|Write]:

7. Enter an access mode for the SNMP community and press Return.

R

Enter R to permit read only access to the SNMP community.

W

Enter W to permit read-write access to the SNMP community.

The following prompt appears:

Enter SNMP Manager IP Addr:

8. Enter an IP address of an SNMP management station to permit it to access the switch. Press Return.

Use the following format for an IP address:

XXX.XXX.XXX.XXX

The default, ALL IP, indicates that all IP addresses are permitted to access the switch. You cannot enter ALL IP at this prompt; however, you can allow access to all IP addresses by pressing Return.

The following prompt appears:

Enter Trap Receiver IP Addr:

9. Enter an IP address that will receive trap messages. Press Return.

Use the following format for an IP address:

XXX.XXX.XXX.XXX

The display at the top of the Configure SNMP Community menu is updated to reflect your changes.

10. After making your changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Changes to the SNMP parameters are immediately activated on the switch.

Deleting a SNMP Community

Use the following procedure to delete a SNMP community.

1. From the Main Menu, type **5** to select System Menu.
The System Menu in Figure 8 on page 48 is displayed.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is displayed in Figure 9 on page 48.
3. From the Configure System window, type **7** to select Configure SNMP.
The Configure SNMP Menu is displayed in Figure 10 on page 49.
4. Select **3** - Configure SNMP Community to configure SNMP parameters.
The Configure SNMP Community menu appears. See Figure 11 on page 50.
5. Select **2** - Delete SNMP Community to remove an SNMP community.
The following prompt appears:
`Enter SNMP Community Name:`
6. Enter a SNMP community name from the list at the top of the menu.
Press return.
A confirmation message is displayed.
7. Enter **Y** to delete the SNMP community.
The display at the top of the Configure SNMP Community menu is updated to reflect your changes.
8. After making your changes, type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.
Changes to the SNMP parameters are immediately activated on the switch.

Modifying a SNMP Community

Use this procedure to change the attributes of a SNMP community.

1. From the Main Menu, type **5** to select System Menu.
The System Menu in Figure 8 on page 48 is displayed.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is displayed in Figure 9 on page 48.
3. From the Configure System window, type **7** to select Configure SNMP.
The Configure SNMP Menu is displayed in Figure 10 on page 49.
4. Select **3** - Configure SNMP Community to configure SNMP parameters.
The Configure SNMP Community menu appears. See Figure 11 on page 50.
5. Select **3** - Modify SNMP Community.
The Modify SNMP Community menu appears.

```

Allied Telesyn AT-8400 Series - AT-S60
Administration Building Switch

Login Privilege: Manager

                          Modify SNMP Community Menu

Community Name Access Mode Status Manager IP Address Trap Receiver IP
-----
Private125      Read|Write  Enabled  192.168.1.101   192.168.1.101
PublicAll178    Read Only   Enabled  192.168.1.201   192.168.1.201

1 - Add Attributes to Community
2 - Delete Attributes from Community
3 - Set Community Access Mode
4 - Set Community Status

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 12 Modify SNMP Community Menu

6. Select **1** - Add Attributes to Community to add SNMP manager and Trap Receiver IP addresses. You can add up to eight IP addresses for SNMP Managers. Additionally, you can add up to eight Trap Receiver IP Addresses.

The following prompt appears:

```
Enter SNMP Community Name:
```

7. Enter a SNMP community name from the list at the top of the menu and press Return. The SNMP community names are case sensitive.

The following prompt appears:

```
Enter SNMP Manager IP Addr:
```

8. Enter an IP address to permit the SNMP manager to access the switch. Press Return.

Use the following format for an IP address:

```
XXX.XXX.XX.XXX
```

Or, to skip this prompt, press Return.

The following prompt appears:

```
Enter Trap Receiver IP Addr:
```

9. Enter an IP address to send trap messages. Press Return.

Use the following format for an IP address:

```
XXX.XXX.XX.XXX
```

Or, to skip this prompt, press Return.

The display at the top of the Configure SNMP Community menu is updated to reflect your changes.

10. Select **2** - Delete Attributes from Community to delete an IP address from the SNMP manager or a trap receiver.

The following prompts appear:

```
Enter SNMP Community Name:
```

```
Enter SNMP Manager IP Addr:
```

See Steps 6 through 8 for information about specifying these attributes. Enter the information and press Return.

A confirmation message appears:

```
Do you want to delete this SNMP Manager?
```

11. Enter **Y** to delete the IP address of this SNMP manager. Enter **N** to retain the IP address of the SNMP manager. Then press Return.

The following prompt appears:

```
Enter the Trap Receiver IP address:
```

12. Enter the Trap Receiver IP address and press return.

The following confirmation message appears:

```
Do you want to delete Trap Receiver IP Address?
```

13. Enter **Y** to delete the IP address of the Trap Receiver. Enter **N** to retain the IP address of the Trap Receiver. Press Return.

14. Select **3** - Set Community Access Mode to change the access mode from read only to read/write or vice versa. Follow the prompts.

15. Select **4** - Set Community Status to enable or disable the current community. Follow the prompts.
16. After making your changes, type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

Changes to the SNMP parameters are immediately activated on the switch.

Displaying a SNMP Community

Use the following procedure to display the attributes of a SNMP community.

1. From the Main Menu, type **5** to select System Menu.
The System Menu in Figure 8 on page 48 is displayed.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is displayed in Figure 9 on page 48.
3. From the Configure System window, type **7** to select Configure SNMP.
The Configure SNMP Menu is displayed in Figure 10 on page 49.
4. Select **4** - Display SNMP Community to display the attributes of an SNMP community. The following menu appears:

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Administration Building Switch

Login Privilege: Manager

                Configure SNMP Community Name
Community Name  Access Mode Status  Manager IP Address  Trap Receiver IP
=====
Private125      Read|Write  Enabled  147.41.11.30        147.45.16.70
                147.45.16.80        147.45.16.80
                147.45.16.81
PublicATI78     Read Only   Enabled  147.41.11.12        147.42.22.22
                147.44.16.86        147.45.16.86
                147.45.16.88        147.45.16.88
                147.45.16.90        147.45.16.90
HighSchool2     Read|Write  Enabled  147.45.10.80        147.45.10.80

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 13 Display SNMP Community Menu

Rebooting a Switch

To reset a switch, perform the following procedure:

1. From the Main Menu, type **4** to select Administrator Menu.
2. From the Administrator Menu, type **B** to select Reboot the switch.

The following prompt is displayed:

```
The switch is about to reboot. Do you want to  
proceed? [Yes/No] ->
```

3. Type **Y** to reset the switch or **N** to cancel this procedure.

If you type **Y**, the following is displayed:

```
Rebooting the Switch...
```

```
.  
.   
.
```

```
Init Done!
```

4. Press the Return key.

The switch reloads its operating system, a task requiring a few minutes to complete.



Caution

The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Configuring the AT-S60 Software Security Features

The AT-S60 software has several security features that can help prevent unauthorized individuals from changing the parameter settings of an AT-8400 switch. The security features are:

- ❑ **Manager and Operator Passwords** - The management software has two standard, management login accounts: Manager and Operator. The Manager account allows you to configure all switch parameters, while the Operator account only allows you to view the parameter settings. The default login password for Manager access is "friend". The default password for Operator access is "operator". The passwords are case-sensitive. For instructions on how to change a password, refer to **Configuring the Management Passwords** on page 57.
- ❑ **Console Timeout** - This parameter causes the management software to automatically end a management session if it does not detect any activity from the local or remote management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the console timeout value is 10 minutes. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 59.
- ❑ **Web Access** - You can disable the web browser management feature on the switch, and so prevent individuals from managing the switch remotely using a web browser. For instructions on how to set this security feature, refer to **Configuring Management Access** on page 59.
- ❑ **SNMP Access** - You can also disable the SNMP management feature on the switch, and so prevent individuals from managing the switch remotely using a SNMP management program. For instructions on how to set this security feature, refer to **Configuring SNMP Community Strings and Trap IP Addresses** on page 47.

Configuring the Management Passwords

There are two levels of management access on an AT-8400 switch: Manager and Operator. When you log in as a Manager, you can view and configure all of a switch's operating parameters. When you log in as an Operator, you can only view the operating parameters; you cannot change any values.

Log in as a Manager or an Operator by entering the appropriate login id and password when you start an AT-S60 management session. The default password for Manager access is "friend". The default password for Operator access is "operator". The passwords are case-sensitive.

To change the Manager or Operator password, perform the following procedure:

1. From the Main Menu, type **4** to select Administrator Menu.
2. From the Administrator Menu, type **7** to select Set Password. The Passwords Menu in Figure 14 is displayed.

```
Allied Telesyn AT-8400 Series - AT-S60
Login Session: Manager
                Passwords Menu

1 - Set Manager Password
2 - Set Operator Password

R - Return to Previous Menu

Enter your selection?
```

Figure 14 Passwords Menu

3. To change the Manager password, type **1**. To change the Operator password, type **2**. Follow the prompts. The password can be from 0 to 20 alphanumeric characters. The passwords are case-sensitive.



Caution

Allied Telesyn recommends that you do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you will be managing the switch from a web browser. Many web browsers do not accept special characters in passwords.

Note

You must assign different values to each password.

Configuring Management Access

To configure the console timer, web access, and SNMP access security features of the AT-S60 management software, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is displayed. See Figure 8 on page 48.
2. Select **1** - Configure System.
The Configure System Menu is displayed. See Figure 9 on page 48.
3. To configure the console timer, type **2** to select Console Disconnect Timer Interval and, when prompted, enter a value of from 1 to 60 minutes. Then press Return. The default is ten minutes.
For example, if you specify 2 minutes, the AT-S60 management software automatically ends a management session if it does not detect any activity from the local or remote management station after 2 minutes.
4. To configure web browser access, type **3** to select Web Server Status and, when prompted, type **E** to enable web access or **D** to disable web access.
For example, if you disable web access, no one will be able to manage the switch remotely using a web browser.
5. To configure SNMP access, type **7** to select Configure SNMP. See **Configuring SNMP Community Strings and Trap IP Addresses** on page 47 for details.
If you disable SNMP access, no one will be able to manage the switch remotely using an SNMP management program.
6. After you have made the desired changes, type **R** twice to return to the Main Menu. Then type **S** to select Save Configuration Changes.
Your changes are immediately activated on the switch.

Viewing the AT-S60 Hardware and Software Information

The procedures in this section display the following switch information:

- ☐ System power information
- ☐ Fan status
- ☐ AT-S60 version number
- ☐ Bootloader version number
- ☐ MAC address

Displaying System Hardware Information

To display the system power and fan information, do the following:

1. Type **5** to select the System Menu from the Main Menu.
The System Menu is displayed in Figure 8 on page 48.
2. Select **2** - Display System Hardware Information to display system power information.

The Display System Hardware Information menu is displayed in Figure 15.

You cannot change the information displayed in selections 1 through 3 in the Display System Hardware Information Menu. These fields are for display purposes only.

```

Allied Telesyn AT-8400 Series - AT-S60
Login Privilege: Manager
Display System Hardware Information

1 - System 3.3V Power..... 3.3V
2 - System 5V Power..... 5.1V
3 - System Temperature ..... 27 C
4 - Display System Fan A Information
5 - Display System Fan B Information

R - Return to Previous Menu
Enter your selection?
```

Figure 15 Display System Hardware Information Menu

3. To display fan information, select **4** - Display System Fan A Information or Select **5** - Display System Fan B Information.

The Display System Fan A Information menu is displayed in Figure 9. The Display System Fan A Information menu is identical to the Display System Fan B Information menu.

You cannot change the information displayed in selections 1 through 6 in the Display System Fan A Information menu. These fields are for display purposes only.

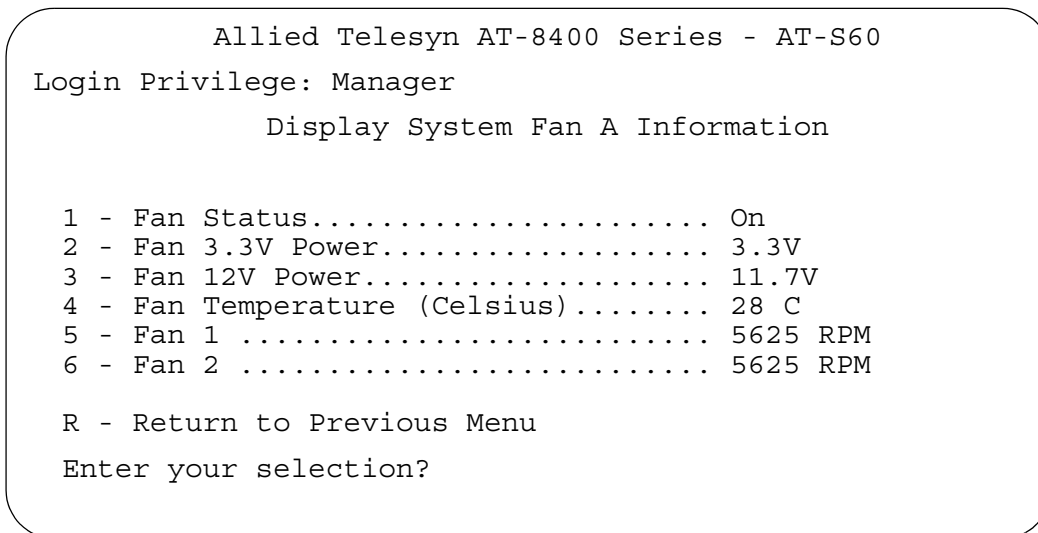


Figure 16 Display System Fan A Information Menu

Displaying System Software Information

To display the system software information, perform the following steps:

1. Select **5** - System Menu from the Main Menu.
The System Menu is displayed in Figure 8 on page 48.
2. Select **3** - Display Software System Information.
The Display System Software Information window is displayed in Figure 15 on page 60.

You cannot change the information displayed in selections 1 through 6 in the Display Hardware System Information Menu. These fields are for display purposes only.

```
Allied Telesyn AT-8400 Series - AT-S60
Login Privilege: Manager
      Display System Software Information

1 - Application Software Version ... ATS60 v1.1.4
2 - Application Software Build Date. Jul 2 2003 08:40:34
3 - Bootloader Version ..... ATS60_LOADER v1.1.0
4 - Bootloader Build Date ..... May 5 2003 09:41:59
5 - MAC Address ..... 00.A0.D2.17.32.00
6 - System Up Time ..... 3 Days 2 Hours 1 Minutes 5 Seconds

R - Return to Previous Menu
Enter your selection?
```

Figure 17 Display System Software Information Menu

Pinging a Remote System

You can instruct the switch to ping a remote device on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.
The Administration Menu is displayed in Figure 3 on page 38.
2. From the Administration Menu, type **P** to select Ping a Remote System.

The following prompt is displayed:

Please enter an IP address ->

3. Enter the IP address of the end node you want the switch to ping and press Return.

The results of the ping command are displayed on the screen. To stop the ping, press any key.

Returning the AT-S60 Software to the Factory Default Values

The procedure in this section returns all AT-S60 software parameters to their default values. This procedure also deletes any VLANs that you have created on the switch.

Note

The AT-S60 software default values can be found in **Appendix A, AT-S60 Default Settings** on page 343.

To return the AT-S60 management software to its default settings, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
2. From the System Menu, type **1** to select Configure System.
The Configure System Window is displayed.
3. Select **D** - Reset to Factory Defaults.
The following prompt is displayed:
Do you want to reset to Factory Defaults? [Yes/No] ->
4. Type **Y** for yes or **N** for no.
The following prompt is displayed:
Do you want to reset IP, Subnet, and Gateway [Yes/No] ->
5. If you type **Y** for yes, all switch parameters including the IP address, subnet mask, and gateway address are changed to their default values. If you type **N** for no, all switch parameters excluding the IP address, subnet mask, and gateway address are changed to their default values.
The following prompt is displayed:
Do you want to reset serial port Baud Rate to 9600 Bps [Yes|No] ->
Type **Y** for yes or **N** for no.
The following prompt is displayed:
Please reboot the switch for the Factory Defaults to take effect.
Switch is about to reboot. Do you want to proceed? [Yes/No] ->
6. Type **Y** to reboot the switch.
The Factory Defaults take effect only after the Switch reboots.
Do you want to Reboot the Switch now? [Yes/No] ->

7. Type **Y** to reboot the switch.

The operating parameters are returned to their default values and the switch is reset.



Caution

The switch will not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Configuring the Console Startup Mode

You can configure the AT-S60 software to display either the Main Menu or the command line interface prompt (#) when you start a local management session. The default is the Main Menu.

To change the console startup mode, perform the following procedure:

1. From the Main Menu, type **5** to select the System Menu.
The System Menu is displayed. See Figure 8 on page 48.
2. From the System Menu, type **1** to select the Configure System Window.
The Configure System Window is displayed. See Figure 9 on page 48.
3. Type **5** to select Console Startup Mode.
You can toggle between the Menu and CLI values. Menu is the default. Select Menu to start a management session with the Main Menu when you log in. Select CLI to start a management session with the Command Line Interface when you log in.
4. Type **R** twice to return to the Main Menu. Then select **S** to save your configuration changes.
Your changes to the console startup mode take effect the next time you start a management session.

Chapter 4

Enhanced Stacking

This chapter explains the enhanced stacking feature and provides procedures for using this feature with a local or Telnet management session. This chapter contains the following sections:

- ❑ **Enhanced Stacking Overview** on page 68
- ❑ **Setting a Switch's Enhanced Stacking Status** on page 71
- ❑ **Selecting a Switch in an Enhanced Stack** on page 73

Enhanced Stacking Overview

The enhanced stacking feature can make it easier for you to manage both AT-8400 and AT-8000 Series switches in your network. It offers the following benefits:

- ☐ You can manage up to 24 switches from one local or remote management session. This eliminates having to initiate a separate management session for each switch in your network. With the AT-8400 switch as the master switch, you can manage AT-8000 Series switches that are configured with the AT-S39 software version 3.1 and above.
- ☐ You can assign an IP address to the master switch. In addition, you can manage slave switches without assigning them individual IP addresses. This feature reduces the number of IP addresses that you need to assign to your network devices for remote management.
- ☐ Remotely managing a new switch in your network is simplified. You simply connect it to your network. Once connected to the network, you can begin to manage it immediately from any workstation in your network.

Guidelines

There are a few guidelines to keep in mind when implementing enhanced stacking for your network:

- ☐ Each subnet in your network constitutes an enhanced stack. You cannot have multiple enhanced stacks in a subnet.
- ☐ All switches that are within an enhanced stack must be in the same management VLAN.
- ☐ Enhanced stacks can be placed in different management VLANs.
- ☐ Each subnet must have at least one master switch. Allied Telesyn recommends you assign two master switches to an enhanced stack.
- ☐ You must assign the master switch an IP address and subnet mask.
- ☐ You must change the master switch's stacking status to Master.
- ☐ The enhanced stacking feature uses the IP address 176.16.16.16. Do not assign this address to any device on your subnet if you intend to use the enhanced stacking feature.

There are three basic steps to implementing this feature on your network:

1. You must select a switch in your network to function as the master switch of the stack.

You can select an AT-8400 or an AT-8000 Series switch to act as the master switch of an enhanced stack. For networks that consist of more than one subnet, there must be at least one master switch in each subnet.

Allied Telesyn recommends that you assign two master switches to each subnet. That way, if you remove one of the master switches from the network, such as for maintenance, you are able to remotely manage the switches in the subnet using the second master switch.

Note

Only switches connected to the management VLAN of the master switch can be discovered and managed through enhanced stacking. Switches that are not connected to the management VLAN will not be discovered even if they are in the same subnet as the master switch.

2. You must assign the master switch an IP address and a subnet mask.

A master switch must have an IP address and subnet mask. The other switches in an enhanced stack, referred to as slave switches, do not.

If your enhanced stack has more than one master switch, you must assign a unique IP address to each master switch.

You can set an IP address manually or activate the BOOTP and DHCP services on a master switch and have the master switch obtain its IP information from a BOOTP or DHCP server on your network. Initially, assigning an IP address or activating the BOOTP and DHCP services can only be performed through a local management session.

Note

For instructions on how to set the IP address manually, refer to **Configuring an IP Address and Switch Name** on page 38. For instructions on activating the BOOTP and DHCP services, refer to **Activating the BOOTP and DHCP Services** on page 45.

3. You must change the enhanced stacking status of the master switch to Master.

This is explained in the procedure **Setting a Switch's Enhanced Stacking Status** on page 71.

Example For an example of the enhanced stacking feature, see Figure 18. This example shows a mixture of AT-8400 and AT-8000 Series switches. With this configuration, starting a local or remote management sessions on either AT-8400 Series master switch, provides management access to the AT-8000 Series switches as well.

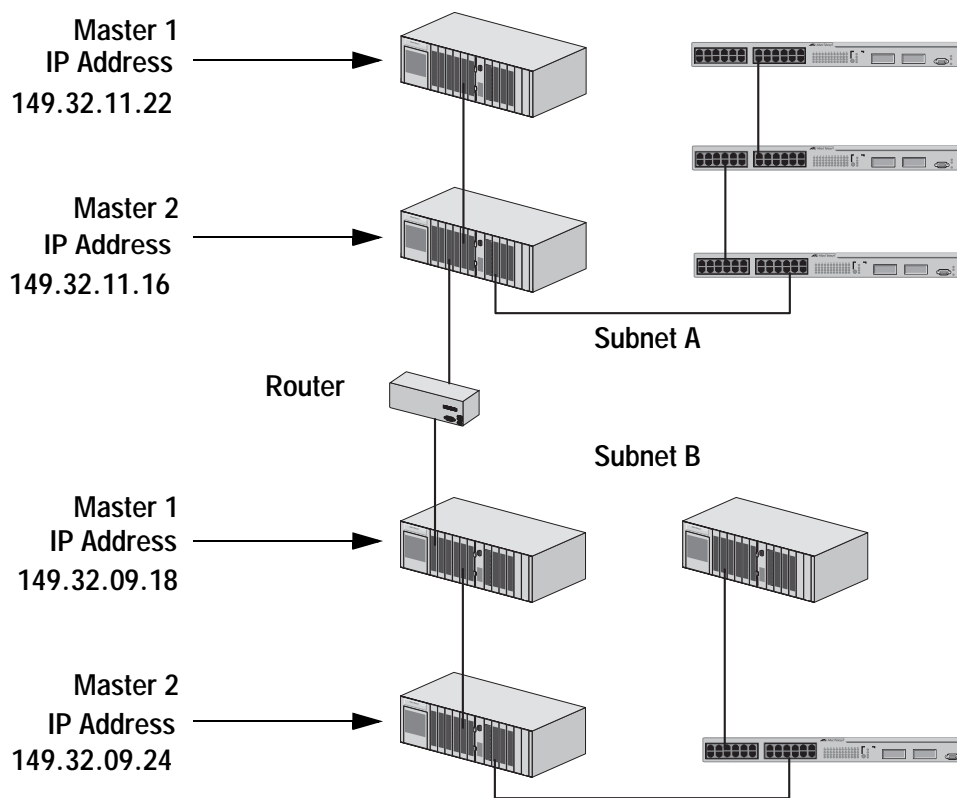


Figure 18 Enhanced Stacking Example

The example shown in Figure 18 consists of a network of two subnets interconnected by a router. Two switches in each subnet have been selected as the master switches of their respective subnets, and each has been assigned a unique IP address.

To manage the switches of a subnet, you start a local management session or a remote Telnet management session with one of the master switches in the subnet. Then, you have management access to all the AT-8400 switches in the same subnet.

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master switch, slave switch, or unavailable. Each status is described below:

- ☐ Master switch - A master switch of a stack can be used to manage all the other switches in a subnet. You can assign the master status to either an AT-8400 or an AT-8000 Series switch which can then be used to manage a mixture of AT-8400 and AT-8000 Series switches. Once you have established a local or remote management session with the master switch, you can access and manage all the switches in the subnet.

A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP services on the switch.

- ☐ Slave switch - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask.
- ☐ Unavailable - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally.

Note

You can use Telnet or the Web to manage a switch with an unavailable stacking status remotely. However, the switch must be directly connected to the AT-8400 and you must assign it a unique IP address.

Note

The default setting for a switch is Slave.

Configuring Enhanced Stacking

To adjust a switch's enhanced stacking status, perform the following procedure:

1. From the Main Menu, type **8** to select Enhanced Stacking.

The Enhanced Stacking menu is displayed in Figure 19.

```

Allied Telesyn AT-8400 Series - ATS60
High School Switch
Login Privilege: Manager
Enhanced Stacking

1 - Switch State- (M)aster/ (S)lave/ (U)navailable.... Master
2 - Stacking Services

R - Return to Previous Menu
Enter your selection?

```

Figure 19 Enhanced Stacking Menu

The menu displays the current status of the switch at the end of selection "1 - Switch State." The default is Slave.

Note

The "2 - Stacking Services" selection in the menu is available only when you set the status to master. For information regarding using this selection, see **Selecting a Switch in an Enhanced Stack** on page 73

2. To change a switch's stacking status, type **1** to select Switch State. The following prompt is displayed.
Enter new setup (M/S/U) ->
3. Type **M** to change the switch to a master switch, **S** to make it a slave switch, or **U** to make the switch unavailable. Press Return.
4. Type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

A change to the status is immediately activated on the switch.

Selecting a Switch in an Enhanced Stack

Before performing a procedure on a switch, check that you are accessing the correct switch. If you assigned system names to your switches, this is a simple check. The name of the switch you are currently managing is displayed at the top of every management menu. For example, in Figure 20, the name of the switch is Sales Switch.

When you start a management session on the Master switch of a subnet, you are, by default, addressing that particular switch. The management tasks that you perform effect only the master switch.

To manage a slave switch or another Master switch in the subnet, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the Main Menu, type **8** to select Enhanced Stacking.
The Enhanced Stacking menu is displayed as shown in Figure 19 on page 72.
2. From the Enhanced Stacking menu, type **2** to select Stacking Services.
The Stacking Services menu is displayed in Figure 20.

```

Allied Telesyn AT-8400 Series - ATS60
Sales Switch

Login Privilege: Manager

Stacking Services

Num  MAC Address      Name      Switch  Software  Switch
-----
1 - Get/Refresh List of Switches
2 - Sort Switches in New Order
3 - Access Switch
4 - Download Image/Bootloader
5 - Download Configuration

R - Return to Previous Menu

```

Figure 20 Stacking Services Menu

3. Type **1** to select Get/Refresh List of Switches.

The Master switch polls the network for all slave and Master switches in the subnet and displays a list of the switches in the Stacking Services menu.

The updated Stacking Services menu is displayed in Figure 21.

```

Allied Telesyn AT-8400 Series - ATS60
Sales Switch

Login Privilege: Manager

Stacking Services

Num  MAC Address      Name      Switch  Software  Switch
-----
1    00:30:84:5b:a2:e0 Sales    Master   v3.1.0    AT-8024GB
2    00:30:84:52:03:80 Finance  Slave   v3.1.0    AT-8024GB
3    00:30:84:c7:6e:20 Finance3 Slave   v3.1.0    AT-8026FC

1 - Get/Refresh List of Switches
2 - Sort Switches in New Order
3 - Access Switch
4 - Download Image/Boot Loader
5 - Download Configuration

R - Return to Previous Menu

Enter your selection?

```

Figure 21 Updated Stacking Services Menu

Note

The Master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

By default, the switches are sorted in the menu by MAC address. You can sort the switches by name as well. This is accomplished with the selection **2** - Sort Switches in New Order.

4. To manage a different switch in an enhanced stack, type **3** to select Access Switch.

A prompt similar to the following is displayed:

```
Enter the switch number -> [1 to 24]
```

5. Type the number of the switch you want to manage. Press Return.
A prompt is displayed if the switch has been assigned a password.
6. Enter the remote switch's login id and press Return.

7. Enter the remote switch's password and press Return.

The default password for Manager access on an AT-8400 switch is "friend". The default password for Operator access is "operator". The passwords are case-sensitive.

The Main Menu of the selected switch is displayed. You now can manage the switch. Any management tasks you perform effect only the selected switch.

Note

Options **4** - Download Image/Boot Loader and **5** - Download Configuration are explained in **Chapter 15, File Downloads and Uploads** on page 225.

8. Type **R** twice to return to the Main Menu. Type **S** to Save configuration changes.

Returning to the Master Switch

When you have finished managing a slave switch and want to manage another switch in the subnet, return to the Main Menu of the slave switch. Then type **S** to save your configuration changes and type **Q** for Quit. This returns you to the Stacking Services menu. Once you see that menu, you are again addressing the Master switch from which you started the management session.

You can select another switch in the list to manage or, if you want to manage the Master switch, return to the master switch's Main Menu by typing **R** twice.

Chapter 5

Port Parameters

The chapter contains procedures for viewing and changing the parameter settings for the individual ports on a switch with a local or Telnet management session. It contains the following procedures:

- ❑ **Displaying Port Status** on page 77
- ❑ **Configuring Port Parameters** on page 81

Displaying Port Status

This section provides a procedure to display the status of a port. To display port statistics, see **Displaying Port Statistics** on page 223.

To display the status of the ports on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

The Port Menu is shown in Figure 22.

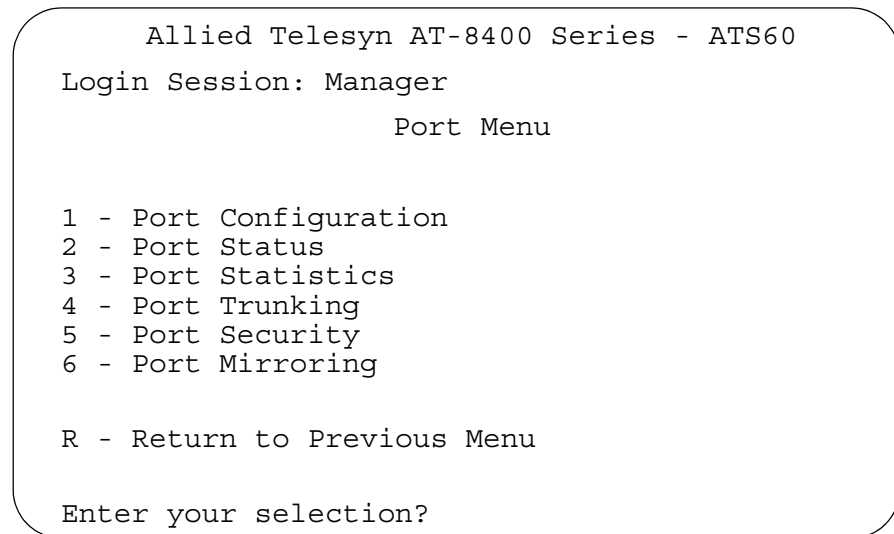


Figure 22 Port Menu

2. From the Port Menu, type **2** to select Port Status.

The Port Status Menu is displayed. See Figure 23.

```

Allied Telesyn AT-8400 Series - AT-S60

Login Session: Manager

Port Status

Port Status  Link Neg  MDI/X  Speed  Duplex PVID  Flow Ctl  STP State  Priority
-----
1.1  Enabled  Up      Auto MDI  0010  Half  0001  Disabled  Forwarding  No
1.2  Enabled  Up      Auto MDI  0100  Full  0001  Disabled  Forwarding  No
1.3  Enabled  Up      Auto MDI  0100  Full  0001  Disabled  Forwarding  No
1.4  Enabled  Up      Auto MDI  0100  Full  0001  Disabled  Forwarding  No
1.5  Enabled  Up      Auto MDI  0010  Half  0001  Disabled  Forwarding  No
1.6  Enabled  Up      Auto MDI  0100  Full  0001  Disabled  Forwarding  No
1.7  Enabled  Up      Auto MDI  0100  Full  0001  Disabled  Forwarding  No
1.8  Enabled  Up      Auto MDI  0010  Half  0001  Disabled  Forwarding  No

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 23 Port Status Menu

The information in this menu is for viewing purposes only. The columns in the menu are described below:

Port

Indicates the port number in the following format:

slot number. port number

Status

Indicates the status, enabled or disabled, of the port.

Enabled - indicates the port will forward traffic.

Disabled - indicates the port will not forward traffic.

Link

The status of the link between the port and the end node connected to the port. Possible values are:

Up - indicates that a valid link exists between the port and the end node.

Down - indicates that the port and the end node have not established a valid link.

Note

The link status between the port and the end node can be displayed as "Up" even after it has been disabled in the Port Configuration menu. For more information on how to configure a port, refer to **Configuring Port Parameters** on page 81.

Neg

The status of Auto-Negotiation on the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.

Manual - Indicates that the operating speed and duplex mode have been set manually.

MDI/X

The operating configuration of the port. Possible values are Auto, MDI, MDI-X. The Auto value indicates that the port is automatically determining the appropriate MDI or MDI-X setting.

Speed

The operating speed of the port. Possible values are:

0010 - Indicates 10 Mbps.

0100 - Indicates 100 Mbps.

1000 - Indicates 1000 Mbps.

Duplex

The duplex mode of the port. Possible values are half-duplex and full-duplex.

PVID

The port VLAN identifier currently assigned to the port.

Flow Ctl

The flow control setting for the port. Possible values are:

Auto - Flow control is automatically activated on the port if the end node connected to the port uses flow control. If the end node is not using flow control, neither will the port.

Enabled - Flow control occurs on both packets entering and leaving the port.

Disabled - No flow control occurs on the port.

STP State

The current operating status of the port. Possible values are:

Forwarding - The port is sending and receiving Ethernet frames. This is the normal state for a switch port.

Disabled - STP operations have been disabled on the port.

Blocking - This is the standby mode. The port does not participate in frame relay. The forwarding process discards received frames and does not submit forwarded frames for transmission.

Listening - The port is enabled for receiving frames only. The port is preparing to participate in frame relay.

Learning - The port is enabled for receiving frames only. The learning process can add new source address information to the forwarding database.

Priority

The priority assigned to packets that are received by the port. Possible values are:

No - Indicates no override priority has been assigned to the port. Untagged packets are forwarded to the low priority queue. Tagged packets are forwarded to either the high or low queue, depending on the priority embedded in the packets.

Low - Indicates low priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the low priority queue.

High - Indicates high priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the high priority queue.

For more information, see **Class of Service Overview** on page 213.

Configuring Port Parameters

To configure the parameter settings for a port on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

The Port Menu is displayed in Figure 22 on page 77.

2. From the Port Menu, type **1** to select Port Configuration.

The following prompt is displayed:

Enter port-list:

3. Enter the number of the port you want to configure and press Return. See **Specifying Ports** on page 26.

The Port Configuration menu is displayed in Figure 24.

```

Allied Telesyn AT-8400 Series - ATS60
Login Session: Manager
Port Configuration

Configuring Port 1.3
0 - Port Name ..... Port_1.3
1 - Status ..... Enabled
2 - Broadcast Filter..... Disabled
3 - Override Priority.... No override
4 - HOL Blocking ..... Disabled
5 - Back Pressure ..... Disabled
6 - Flow Control ..... Auto
7 - Negotiation ..... Auto

D - Set Default Port Configuration
R - Return to Previous Menu

Enter your selection?
```

Figure 24 Port Configuration Menu

Note

The sample Port Configuration Menu in the figure above is for a 10/100 Mbps twisted pair port. The menu for a fiber optic port or a GBIC module contains a subset of the parameters.

4. Adjust the port parameters as desired. You adjust a parameter by typing its number. This toggles the parameter through its possible settings. The parameters are described below.

0 - Port Name

This parameter only appears if you entered one port to configure. It indicates the name of the port you are currently viewing.

1 - Status

You use this selection to enable or disable a port. When disabled, a port will not forward frames.

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

Press **6** to toggle between the following settings:

Enabled - The port will forward packets. This is the default setting.

Disabled - The port will not forward packets.

2 - Broadcast Filter

You use this selection to protect a port from a deluge of packets caused by a broadcast storm. Enabling the broadcast filter parameter on a port causes the port to drop broadcast frames.

Press **2** to toggle between the following settings:

Enabled - When a port receives a broadcast frame, the port drops the frame.

Disabled - The port will not watch for broadcast frames. Instead, it accepts broadcast frames. This is the default.

3 - Override Priority

You use this selection to determine packet priority. For information about override priority, see **Class of Service Overview** on page 213.

Press **3** to toggle between the following settings:

No override - Indicated that no override priority is assigned to incoming packets. Instead, the port forwards packets according to the priority embedded in the packet. This is the default.

Low Priority - Indicates low priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the low priority queue.

High Priority - Indicates high priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the high priority queue.

4 - HOL Blocking

You use this selection to prevent a packet from being forwarded to a blocking or blocked port. For example, a blocking or blocked port can be one that is receiving too many packets.

Press **4** to toggle between the following settings:

Enabled - Indicates HOL blocking is turned on. Packets sent from this port will not be forwarded to a blocked port.

Disabled - Indicated HOL blocking is turned off. Packets sent from this port are not prevented from being forwarded to a blocked port. This is the default.

5 - Back Pressure

You can use this selection only if the port or ports you specified are operating at half-duplex mode. When you specify that a port is in this mode and it has a packet that is pending transmission, the port uses the JAM signal when its buffer is full to prevent the end node from sending any more packets.

Press **5** to toggle between the following settings:

Enabled - Indicates back pressure is activated on this port. When the port is receiving too many packets, the port will send a signal to the end node to stop sending information.

Disabled - Indicates back pressure is not activated on this port. When the port is receiving too many packets, the port will not send a signal to the end node to stop sending information. This is the default.

Note

The Auto setting is not available if you set a port's speed and duplex mode manually.

6 - Flow Control

Flow control applies only to ports operating in full-duplex mode. The switch uses a special pause packet when its buffer is full to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.

Press **6** to toggle between the following settings:

Auto - Indicates the port conforms to the flow control setting of the end node. For example, if flow control is active on the end node then flow control is active on this port. Also, if flow control is not active on the end node, then flow control is not active on this port. This is the default.

Disabled - Indicates that no flow control occurs on the port.

Enabled - Indicates that flow control occurs on the port.

7 - Negotiation

You use this selection to configure a port for Auto-Negotiation or to manually set a port's speed and duplex mode.

Press **7** to toggle between the following settings:

Auto - Select Auto (for Auto-Negotiation) to set both speed and duplex mode for the port automatically. This is the default setting.

Manual - Select Manual to set the speed and duplex for the port.

If you select Manual, two additional selections are displayed in the Port Configuration menu:

```
8 - Speed ..... 0100
9 - Duplex .....Full
```

You use these two selections to set the port's speed and duplex mode. The possible settings for the **8** - Speed selections are:

0010 - Indicates 10 Mbps.

0100 - Indicates 100 Mbps.

1000 - Indicates 1000 Mbps. This value only appears if a port is a GBIC port such as on the AT-8413 G/BT line card.

The possible settings for **9** - Duplex are:

Full - Indicates full-duplex mode

Half - Indicates half-duplex mode

D - Set Default Port Configuration

Use this selection to reset the port parameters to their default values. The port parameter defaults are illustrated in Figure 24 on page 81.

5. Once you have set the port parameters, type **R** twice to return to the Main Menu. Then type **S** to Save Configuration Changes.

Configuration changes are immediately activated on a port.

Chapter 6

Port Security

This chapter describes port security and provides the procedures for setting port security with a local or Telnet management session. It contains the following sections:

- ❑ **Port Security Overview** on page 86
- ❑ **Configuring Port Security** on page 88

Port Security Overview

The port security feature can enhance the security of your network. You can use the feature to control which end nodes can forward frames through the switch.

There are four levels of port security:

- ☐ Automatic
- ☐ Limited
- ☐ Secured
- ☐ Locked

You can set port security on a per port basis. Only one security level can be active on a port at a time.

Automatic

The Automatic security mode disables port security on a port. In this mode, a port can learn up to 256 dynamic MAC addresses. This is the default security level for a port.

A dynamic MAC address learned by a port operating with this security level is deleted from the MAC address table if the end node becomes inactive. This prevents the table from becoming full of MAC addresses of inactive nodes. The length of time an inactive dynamic MAC address can remain in the table is determined by the MAC aging time.

Limited

The Limited security level allows you to specify the maximum number of dynamic MAC addresses a port can learn. Once a port has learned its maximum number of addresses, it discards all ingress frames with source MAC addresses not already learned.

When the Limited security mode is activated on a port, all dynamic MAC addresses learned by the port are deleted from the MAC address table. The port then begins to learn new addresses, up to the maximum allowed.

A dynamic MAC address learned on a port operating in the Limited security mode is never timed out from the MAC address table, even when the corresponding end node is inactive. Once the port has learned its maximum number of addresses, it will not learn any new addresses, even when end nodes are inactive.

Static MAC addresses are retained by the port and are not included in the count of maximum dynamic addresses. You can add more static MAC addresses to a port even if the port has already learned its maximum number of dynamic MAC addresses.

Secured The Secured security level instructs a port to forward frames using only static MAC address. The port will not learn any dynamic MAC addresses and will delete any dynamic addressees that it has already learned. Only those end nodes whose MAC addresses have been entered as static addresses will be able to forward frames through the port.

You must enter, either before or after you activate this security level, the static MAC addresses of the end nodes that are allowed to forward frames through the port.

Locked The Lock security level causes a port to immediately stop learning new dynamic MAC addresses. Frames are forwarded using the dynamic MAC addresses that the port has already learned and any static MAC addresses assigned to the port.

Dynamic MAC addresses learned by the port prior to the activation of this security level are never timed out from the MAC address table, even when the corresponding end nodes are inactive. However, the port will not learn new dynamic addresses.

You can add new static MAC addresses to a port operating with this security level.

Note

For background information on MAC addresses and the MAC aging time, refer to **MAC Address Overview** on page 201.

Security Violations and Intrusion Actions

When you set a port's security level, you can also set the action a port performs in the event it receives an invalid frame. This is referred to as intrusion (intruder) action.

Before defining the intrusion actions, it can help to understand first what constitutes an invalid frame. This differs for each security level, as explained here:

- ☐ Limited Security Level - An invalid frame for this security level is an ingress frame with a source MAC address not already learned by a port after the port had reached its maximum number of dynamic MAC addresses. Also, a MAC address that was not assigned to the port as a static address is considered an invalid frame.
- ☐ Secured Security Level - An invalid frame for this security level is an ingress frame with a source MAC address that was not entered as a static address on the port.
- ☐ Locked - An invalid frame for this security level is an ingress frame with a source MAC address that the port has not already learned or that was not assigned as a static address.

You can configure what a port will do if it receives an invalid frame. Here are the options:

- ☐ Discard the invalid frame.
- ☐ Discard the invalid frame and send a trap.
- ☐ Discard the invalid frame, send a trap, and disable the port.

Configuring Port Security

To configure port security, do the following:

To set a switch's port security level, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is displayed in Figure 22 on page 77.
2. From the Port Menu, type **5** to select Port Security.
The Port Security Menu is displayed in Figure 25.

```

Allied Telesyn AT-8400 Series - AT-S60
Login Privilege: Manager
Port Security
1 - Configure Port Security
2 - Display Port Security

R - Return to Previous Menu

Enter your selection?
```

Figure 25 Port Security Menu

3. Type **1** to select Configure Port Security.
The following prompt is displayed:
Enter port-list:
4. Enter the port(s) you want to configure. Then press Return.
For information about how to specify ports, see **Specifying Ports** on page 26.

The Configure Port Security Menu is displayed in Figure 26.

```

Allied Telesyn AT-8400 Series - AT-S60
Login Privilege: Manager
      Configure Port Security
Configuring Port Security 3.1-2
1 - Security Mode ..... Automatic

D - Set Default Port Security
R - Return to Previous Menu

Enter your selection?

```

Figure 26 Configure Port Security Menu

- Press **1** to change the port security on your specified port list.

The following prompt appears:

```
Enter new mode (A-Automatic, L-Limited, S-Secured,
K-lockEd):
```

- Select the desired security level by typing the corresponding letter and then pressing Return. For definitions of the security levels, refer to **Port Security Overview** on page 86.

If you selected Automatic, which disables port security, return to the Main Menu to save your changes.

If you selected one of the other security levels, several new menu options are added to the Configure Port Security menu, as shown here.

```

Allied Telesyn AT-8400 Series - AT-S60
      Configure Port Security 3.1-2
1 - Security Mode ..... Limited
2 - Intrusion Action ..... Discard
3 - Port Participating ..... No
4 - MAC Limit ..... 100

D - Set Default Port Security
R - Return to Previous Menu

Enter your selection?

```

Figure 27 Configure Port Security Menu

Note

Option 4 - MAC Limit appears only for the Limited security level.

7. To set the intrusion action for the port, do the following:

- a. Type **2** to select Intrusion Action.

The following prompt appears:

```
Enter intrusion action: (N-No Action(Discard), T-Trap, D-Disable):
```

- b. Select the desired intrusion action:

N - No Action (Discard): The port discards an invalid frame. This is the default.

T - Trap: The port discards an invalid frame and sends a trap.

D - Disable: The port discards an invalid frame, sends a trap, and disables the port.

8. If you want to enable or disable port security on the port, type **3** to select Port Participating.

Typing **3** toggles the selection through its two options of Yes and No. If you select No, the port operates in the Automatic security level. If you select Yes, the port operates in the security mode that you selected with the **1** - Security Mode option.

Note

Security is activated on a port when you change the Port Participating menu option to Enabled. If you are configuring a port for the Limited security mode, you may want to perform this step after Step 9, where you set the maximum number of dynamic MAC addresses you want the port to learn.

9. If you selected the Limited security mode for the port, do the following to specify the maximum number of dynamic MAC addresses you want the port to be able to learn:

- a. Type **4** to select MAC Limit.

The following prompt appears:

```
Enter port security threshold: [1 to 256] -> 100
```

- b. Enter the maximum number of dynamic MAC addresses you want the port to be able to learn. The range is 1 to 256. The default is 100.

Note

The **D** - Select Default Port Security option in the menu sets the security mode for the port to the default value of Automatic.

10. Return to the Main Menu and type **S** to select Save Configuration Changes.
11. If you configured a port for Secure security level, remember to enter the static MAC addresses of the end nodes that can send packets through the port. For instructions on how to add static MAC addresses, refer to **Adding Static MAC Addresses** on page 207.

Chapter 7

Port Trunking

This chapter describes port trunking and contains the procedures for creating, deleting, and modifying port trunks with a local or Telnet management session. It contains the following sections:

- ❑ **Port Trunking Overview** on page 93
- ❑ **Creating a Port Trunk** on page 97
- ❑ **Deleting a Port Trunk** on page 99
- ❑ **Modifying a Port Trunk** on page 100

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between two Ethernet switches. For the AT-8400 Series switch, a port trunk can consists of up to eight ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between switches and is useful in situations where a single physical data link between switches is insufficient to handle the traffic load.

A port trunk sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

The example in Figure 28 consists of a 1,000 Mbps port trunk with four data links between two AT-8400 switches.

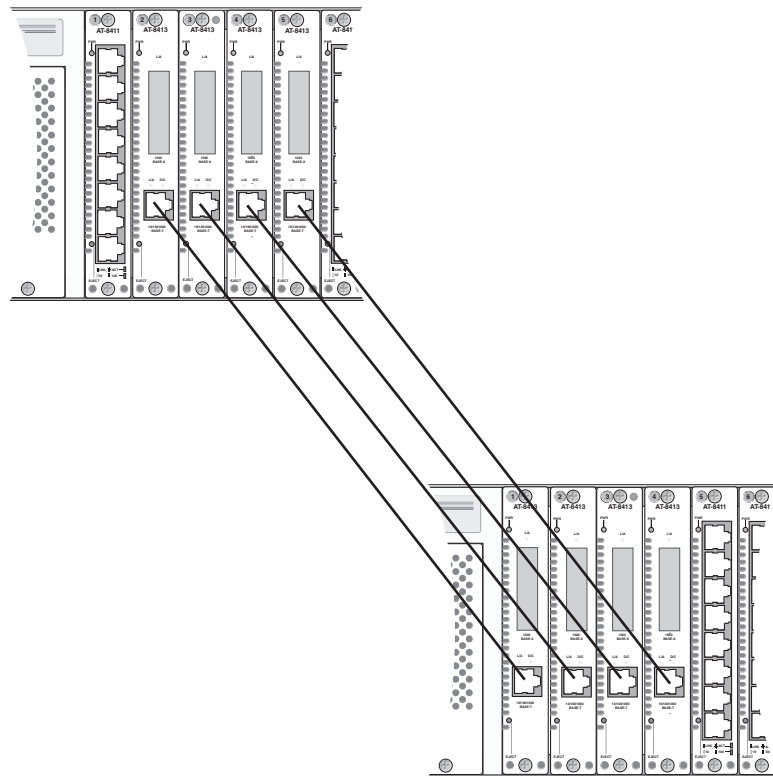


Figure 28 Port Trunk Example with 1000 Mbps Ports

The example in Figure 29 illustrates a 10/100 port trunk with 8 data links between two AT-8400 switches.

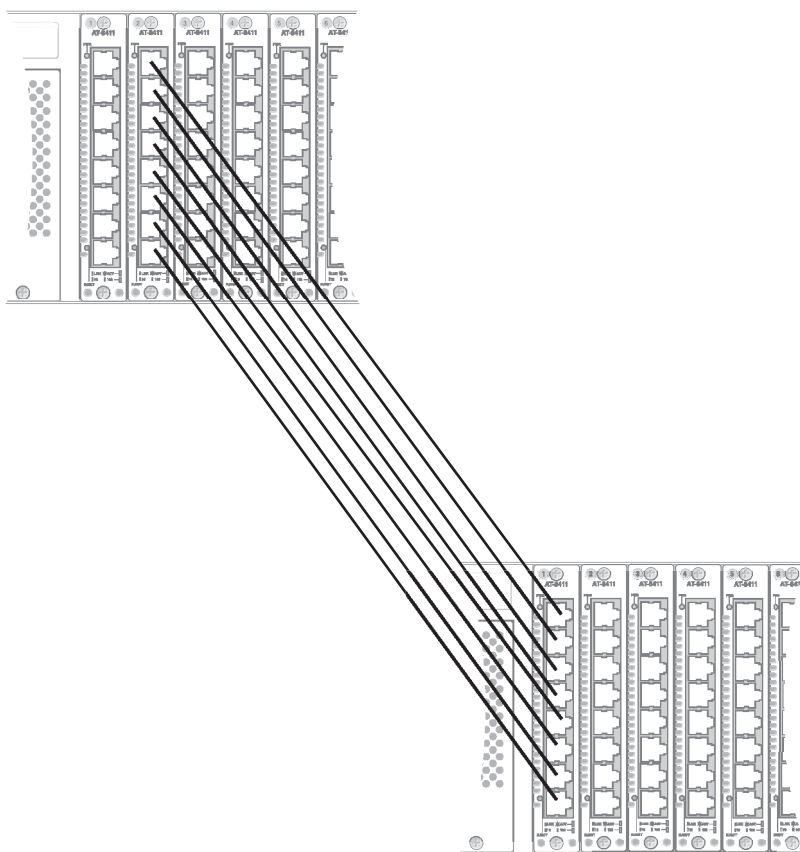


Figure 29 Port Trunk Example with 10/100 Mbps Ports

In addition, you can create a port trunk between an AT-8400 switch and other switches that support trunking.

Port Trunking Guidelines

When creating a port trunk, you need to follow a set of guidelines.

Observe the following guidelines when creating a port trunk:

- ☐ An AT-8400 switch can support up to 8 trunks at a time.
- ☐ A port trunk can consist of a maximum of 8 ports.
- ☐ The ports of a port trunk must be of the same medium type. For example, they can be all twisted-pair ports or all fiber optic ports.
- ☐ For 10/100 port trunks, such as those on an AT-8411 TX line card, all ports included in the trunk must reside on the same line card. See Figure 29 on page 94 for an illustration of a 10/100 Mbps port trunk.

- ❑ For 1,000 Mbps port trunks, such as those on an AT-8413 line card, all ports included in the trunk must reside on different line cards. Generally, there is one 1,000 Mbps port per line card as with the AT-8413 line card. See Figure 28 on page 93 for an illustration of a 1,000 Mbps port trunk.
- ❑ Although each AT-8413 line card contains two ports, only one port can be active at a time. Each AT-8413 line card can forward traffic on either the twisted pair or fiber optic port. When creating a port trunk with AT-8413 line cards, the trunked ports must be made up of either twisted pair or fiber optic ports.
- ❑ The speed, duplex mode, and flow control settings must be the same for all the ports in a trunk. In addition, the broadcast filter, override priority, HOL blocking, back pressure, MDI/MDIX, and negotiation settings must be the same for all the ports in a trunk.
- ❑ The ports of a port trunk must be members of the same VLAN. A port trunk cannot consist of ports from different VLANs.
- ❑ The ports of a port trunk must all have the same security setting.
- ❑ When cabling a trunk, the order of the connections should be maintained on both nodes. The lowest numbered port in a trunk on the switch should be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port on the switch should be connected to the next lowest numbered port on the other device, and so on.

For example, assume that you are connecting a trunk between two AT-8400 switches. On the first AT-8400 switch you chose ports 1.2, 1.3, 1.4, 1.5 for the trunk. On the second AT-8400 switch you chose ports 2.1, 2.2, 2.3, and 2.4. To maintain the order of the port connections, you would connect port 1.2 on the first AT-8400 switch to port 2.1 on the second AT-8400 switch, port 1.3 to port 2.2, and so on.

- ❑ You can create a port trunk using the fiber optic ports in an AT-8412/SC FX line card.

Before Creating Port Trunks

As mentioned in the above guidelines for creating port trunks, you need to ensure the settings on your ports are identical before adding them to a port trunk. To display your current port settings, see **Displaying Port Status** on page 77. Then, to update the port configuration so all of the ports in the trunk have the same configuration, see **Configuring Port Parameters** on page 81. For information about changing port security, see **Configuring Port Security** on page 88.

Load Distribution Methods

The AT-S60 management software provides the Source Address (SA) Trunking load distribution method. When a switch receives a packet from a network node, it examines the destination address to determine on which port, if any, the packet should be transmitted. If the packet is destined for a port trunk, the switch examines the source address of the packet. If this is the first packet from the source node to be transmitted over a port trunk, then the switch assigns the source address to a trunk link. All subsequent packets from the source node are sent from the assigned data link of the trunk.

The switch assigns source addresses so as to evenly distribute the addresses, as much as possible, across all the ports of the trunk. The intent is to ensure all the links in the trunk are used.

Creating a Port Trunk

This section contains the procedure for creating a port trunk on the switch. The ports that you use to create your port trunk must all have the same settings. For more detail, be sure to review the guidelines in **Port Trunking Overview** on page 93 before performing the procedure. Once you create a port trunk, you need to save your new configuration using the **S** - Save Configuration Changes selection on the Main Menu.



Caution

Do not connect the cables to the trunk ports on the switches until after you have configured the trunk with the management software. Connecting the cables before configuring the software will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

To create a port trunk, perform the following procedure:

- 1. From the Main Menu, type **1** to select Port Menu.
- 2. From the Port Menu, type **4** to select Port Trunking.

The Port Trunking menu in Figure 30 is displayed.

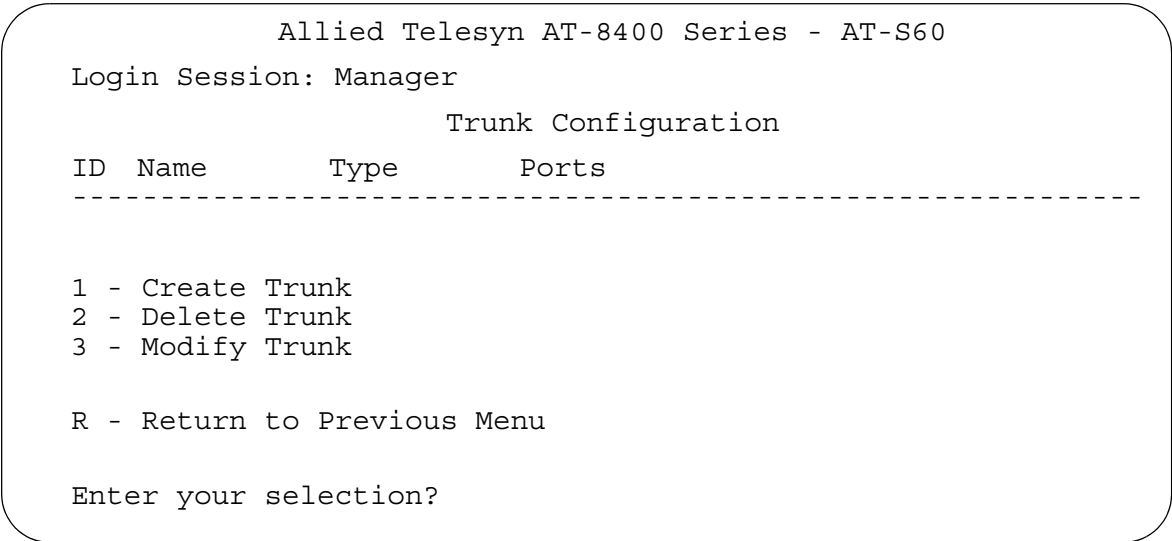


Figure 30 Trunking Configuration Menu

3. Type **1** to select Create Trunk.

The following prompt is displayed.

```
Enter Trunk Name: ->
```

4. Enter an alphanumeric name that identifies the trunk, such as universitytrunk7. Press Return.

You can select a name with a maximum of 16 alphanumeric characters. In addition, the trunk name must contain one alphabetic character. Trunk names must be unique. You cannot enter a port name for this parameter.

The following prompt appears:

```
Enter Trunk Type: (1 - 10/100, 2 - GB): [1 to 2]
```

5. Enter a trunk type based on the speed of the ports and press Return.

Enter **1** for 10/100 Mbps ports.

Enter **2** for GBIC port or a port with speeds of up to 1,000 Mbps.

The following prompt appears:

```
Enter Trunk Ports:
```

6. Enter the ports that will constitute the port trunk and press Return.

For information about how to specify ports, see **Specifying Ports** on page 26.

For 10/100 Mbps port trunks, all the ports that comprise the trunk must be on the same line card.

For 1,000 Mbps port trunks, all the ports that make up the trunk must be on different line cards.

Once you have specified the ports of the trunk, the following message is displayed:

```
Please wait while Trunk is being created...Done!
New ID = 1
```

The Trunk Configuration menu is updated with information about the new trunk.

7. Type **R** twice to reach the Main Menu. Type **S** to select Save Configuration Changes.
8. Configure the ports on the remote switch for port trunking.

9. Connect the cables to the ports of the trunk on the switch.

The port trunk is ready for network operation.

Deleting a Port Trunk

Use this procedure to delete an existing port trunk, including the trunk ID, name, and ports associated with the port trunk. Once you delete a port trunk, you need to save your new configuration using the **S** - Save Configuration Changes selection on the Main Menu.



Caution

Disconnect the cables from the port trunk on the switch before performing the following procedure. Deleting a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

To delete a port trunk from the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

The Port Menu is displayed.

2. From the Port Menu, type **4** to select Port Trunking.

The Trunking Configuration menu is displayed as shown in Figure 30 on page 97.

3. Type **2** to delete a trunk.

The following prompt is displayed:

```
Enter Trunk ID: [1 to 22] -> 1
```

4. Enter the trunk ID number of the port trunk you want to delete and press Return.

After you delete a trunk, the following message is displayed:

```
Please wait while Trunk is being deleted...Done!  
Press any key to continue
```

5. Type **R** two times to reach the Main Menu. Type **S** to select Save Configuration Changes.

You have successfully deleted the port trunk from the switch.

Modifying a Port Trunk

Use this procedure to modify an existing port trunk. See the **Port Trunking Guidelines** on page 94 for information specific to 10/100 Mbps and 1000 Mbps port trunks.

When you select the Modify Port Trunk selection on the Port Trunking menu, you can perform the following actions:

- ☐ Changing the name of the trunk
- ☐ Adding ports to a trunk
- ☐ Deleting ports from a trunk
- ☐ Setting (or overwriting) the ports in a trunk
- ☐ Clearing (or removing) all the ports in a trunk

After you modify a port trunk, you need to return to the Main Menu and save your changes using the **S** - Save Configuration Changes selection.

To modify a port trunk on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **4** to select Port Trunking.

The Trunk Configuration menu is displayed as shown in Figure 30 on page 97.

3. Type **3** - Modify Trunk to modify a port trunk.

The Modify Trunk menu is displayed as shown in Figure 31. Notice the two current port trunks, called **highschool** and **elementary**, included in this Figure.

```

Allied Telesyn AT-8400 Series - AT-S60

Login Session: Manager

                                Modify Trunk

ID Name                        Type      Ports
-----
1   highschool                 10/100MB  4.1-4
2   elementary                 10/100MB  4.5-8

1 - Change Trunk Name
2 - Add ports to Trunk
3 - Delete ports from Trunk
4 - Set ports in Trunk
5 - Clear ports in Trunk

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 31 Modify Trunk Menu

4. Select one of the following options:

Select **1** - Change Trunk Name to change the alphanumeric name of the trunk. See **Changing the Name of the Port Trunk** on page 102.

Select **2** - Add ports to Trunk to add ports to a trunk. See **Adding Ports to an Existing Port Trunk** on page 102.

Select **3** - Delete ports from Trunk to delete ports from a trunk. See **Deleting Ports from a Port Trunk** on page 104.

Select **4** - Set ports in Trunk to overwrite the ports in the trunk with a new list of ports. See **Setting Ports in a Trunk** on page 105.

Select **5** - Clear ports in Trunk to delete all the ports in a trunk. See **Clearing Ports in a Port Trunk** on page 106.

5. Type **R** until you reach the Main Menu. Type **S** to select Save Configuration Changes.

Changing the Name of the Port Trunk

Use this procedure to change the name of an port trunk. Once you change the name of a port trunk, you need to save your new configuration using the **S** - Save Configuration Changes selection on the Main Menu.

To change the name of an port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **4** to select Port Trunking.

The Trunk Configuration menu is displayed as shown in Figure 30 on page 97.

3. Type **3** to modify a trunk.

The Modify Trunk menu is displayed as shown in Figure 31 on page 101.

4. Select **1** - Change Trunk Name to change the alphanumeric name of the trunk.

The following prompt appears:

```
Enter Trunk ID: [1 to 22] -> 1
```

5. Enter the trunk ID number of the trunk you want to change the name of and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 31 on page 101.

After you enter the trunk ID, the following prompt appears:

```
Enter new trunk name:
```

6. Type in a new name and press Return.

You can select a name with a maximum of 16 alphanumeric characters. In addition, the trunk name must contain one alphabetic character. Trunk names must be unique. You cannot enter a port name for this parameter.

The Modify Trunk menu is updated with the new trunk name.

7. Type **R** until you return to the Main Menu. Type **S** - Save Configuration Changes to save the new trunk name

Adding Ports to an Existing Port Trunk

Use this procedure to add ports to an existing port trunk. Be sure to follow the guidelines regarding port trunks. For detailed information, see **Before Creating Port Trunks** on page 95. If you want to overwrite all of the current ports in port trunk and replace them with new ports, see **Setting Ports in a Trunk** on page 105.

Once you add ports to a port trunk, you need to save your new configuration using the **S** - Save Configuration Changes selection on the Main Menu.

To add ports to an existing port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **4** to select Port Trunking.
The Trunk Configuration menu is displayed as shown in Figure 30 on page 97.
3. Type **3** to modify a trunk.
The Modify Trunk menu is displayed as shown in Figure 31 on page 101.
4. Select **2** - Add ports to Trunk to add ports to an existing trunk.
The following prompt appears:
`Enter Trunk ID: [1 to 22] -> 1`
5. Enter the trunk ID number of the trunk you want to modify and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 31 on page 101.
The following prompt appears:
`Enter ports to add to trunk:`
6. Enter the ports you want to add to the trunk and press Return.
For information about how to specify ports, see **Specifying Ports** on page 26.
For 10/100 port trunks, all the ports that comprise the trunk must be on the same line card.
For GBIC port trunks (or ports with speeds up to 1,000 Mbps), all the ports that make up the trunk must be on different line cards.
The Modify Trunk menu is updated with the new ports.
7. Type **R** until you return to the Main Menu. Type **S** - Save Configuration Changes to save the new ports.

Deleting Ports from a Port Trunk

Use this procedure to delete ports from an existing port trunk. If you want to delete all the ports from an existing port trunk and replace them with a new set of ports, see **Clearing Ports in a Port Trunk** on page 106. Once you delete ports, you need to save your new configuration using the **S** - Save Configuration Changes selection on the Main Menu.

To delete a port from a port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **4** to select Port Trunking.

The Trunk Configuration menu is displayed as shown in Figure 30 on page 97.

3. Type **3** - Modify Trunk.

The Modify Trunk menu is shown in Figure 31 on page 101.

4. Select **3** - Delete ports from Trunk.

The following prompt appears:

```
Enter Trunk ID: [1 to 22] -> 1
```

5. Enter the trunk ID number of the trunk you want to modify and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 31 on page 101.

After you enter the trunk ID, the following prompt appears:

```
Enter ports to delete:
```

6. Enter the ports you want to delete from the trunk and press Return.

For information about how to specify ports, see **Specifying Ports** on page 26.

For 10/100 port trunks, all the ports that comprise the trunk must be on the same line card.

For GBIC port trunks (or ports with speeds up to 1,000 Mbps), all the ports that make up the trunk must be on different line cards.

The Modify Trunk menu is updated to reflect the ports you deleted.

7. Type **R** until you return to the Main Menu. Type **S** - Save Configuration Changes to save your changes.

Setting Ports in a Trunk

Use this procedure to overwrite or replace the current ports in a port trunk with a new list of ports. To add ports to an existing port trunk while retaining the current ports, see **Adding Ports to an Existing Port Trunk** on page 102.

Once you have replaced the ports with new ports, you need to save your new configuration using the **S** - Save Configuration Changes selection on the Main Menu.

To overwrite the current ports in a port trunk with a new list of ports, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **4** to select Port Trunking.

The Trunk Configuration menu is displayed as shown in Figure 30 on page 97.

3. Type **3** - Modify Trunk.

The Modify Trunk menu is displayed as shown in Figure 31 on page 101.

4. Type **4** - Set ports in Trunk.

The following prompt appears:

```
Enter Trunk ID: [1 to 22] ->1
```

5. Enter the trunk ID number of the trunk you want to update and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 31 on page 101.

After you enter the trunk ID, the following prompt appears:

```
Enter trunk ports:
```

6. Enter the new trunk ports that will overwrite the current port trunks and press Return.

For information about how to specify ports, see **Specifying Ports** on page 26.

For 10/100 port trunks, all the ports that comprise the trunk must be on the same line card.

For GBIC port trunks (or ports with speeds up to 1,000 Mbps), all the ports that make up the trunk must be on different line cards.

The Modify Trunk menu is updated with the new ports.

7. Type **R** until you return to the Main Menu. Type **S** - Save Configuration Changes to save the new ports.

Clearing Ports in a Port Trunk

Use this procedure to clear, or delete, all of the current ports in a port trunk while leaving the port trunk ID, name, and type. To delete selective ports, see **Deleting Ports from a Port Trunk** on page 104. Once you have deleted all the ports on the trunk, you need to save your new configuration using the **S** - Save Configuration Changes selection on the Main Menu.

To clear or delete all the ports on a port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **4** to select Port Trunking.
The Port Trunking menu is displayed in Figure 30 on page 97.
3. Type **3** - Modify Trunk.
The Modify Trunk menu is displayed in Figure 31 on page 101.
4. Type **5** - Clear ports in Trunk to remove the current list of ports.
The following prompt appears:
Enter Trunk ID: [1 to 22] -> 1
5. Enter the trunk ID number and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 31 on page 101.
After you enter the trunk ID, the following message appears:
Please wait while clearing Trunk ports...Done!
Press any key to continue
The Modify Trunk menu is updated to show no ports associated with the Trunk ID.
6. Type **R** until you return to the Main Menu. Type **S** - Save Configuration Changes to save your changes.

Chapter 8

Port Mirroring

This chapter describes port mirroring and provides the procedures for creating and deleting a port mirror using a local or Telnet management session. It contains the following sections:

- ❑ **Port Mirroring Overview** on page 108
- ❑ **Creating a Port Mirror** on page 109
- ❑ **Modifying a Source Port Mirror** on page 111
- ❑ **Deleting a Destination Port Mirror** on page 113
- ❑ **Enabling a Destination Port Mirror** on page 114
- ❑ **Disabling a Destination Port Mirror** on page 115

Port Mirroring Overview

The port mirroring feature allows you to unobtrusively monitor the traffic on one or more ports by copying the traffic to another port which is called the destination mirror port. Using port mirroring, you can connect a network analyzer to the mirror port to monitor both traffic received and transmitted from one or more ports (which are called source mirror ports). In the software, the destination mirror port is called the destination port while the source mirror ports are called source ports.

Observe the following guidelines when creating a port mirror:

- ☐ You can mirror from one to 12 ports on a switch at a time, depending on number and types of line cards installed in your chassis. However, the more ports you mirror, the less likely the mirroring port can handle all the traffic. For example, if you mirror the traffic of six heavily active ports, the mirror port is likely to drop packets, meaning that it will not provide an accurate mirror.
- ☐ The ports that are mirrored and the mirroring port must be located on the same switch.
- ☐ You can assign each line card one source mirroring port and one destination mirroring port. Each line card can participate in only one port mirror.
- ☐ The ports that are mirrored and the mirroring port must operate at the same speed. For example, you cannot use a 10/100 Mbps port to mirror traffic on a 1000 Mbps GBIC port.

Creating a Port Mirror

Use the following procedure to create a port mirror. For information about how to specify a port, see **Specifying Ports** on page 26. To save your configuration changes, return to the Main Menu and select **S** - Save configuration Changes.

To create a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 22 on page 77.
2. From the Port Menu, type **6** to select Port Mirroring.
The Port Mirroring menu is displayed in Figure 32.

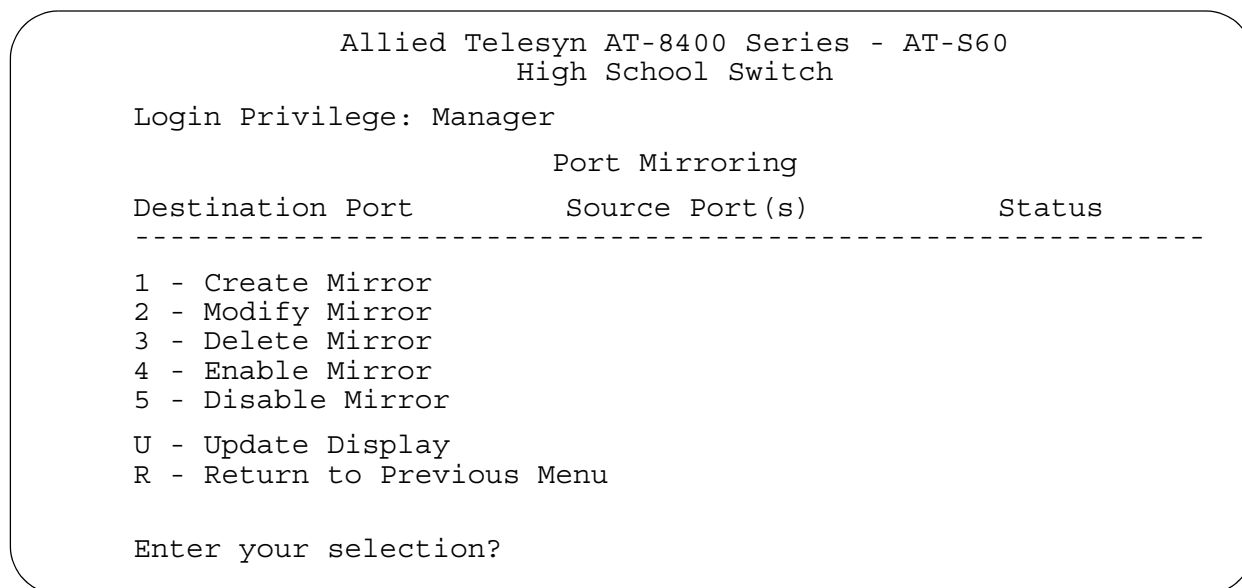


Figure 32 Port Mirroring Menu

3. Type **1** to select Create Mirror.
The following prompt is displayed:
Enter Destination Port:
4. Enter the number of the port that functions as the mirror port (that is, the port where the traffic is copied) and press Return.
You can specify only one mirror port. For information about how to specify a port, see **Specifying Ports** on page 26.
5. The following prompt is displayed:
Enter the Source Port(s) [port-list]:

Enter a single port or a list of nonconsecutive ports on different line cards whose traffic will be mirrored. Press Return.

Note

You cannot assign a range of ports on the same line card as source mirror ports.

The source mirror port (or ports) is displayed at the top of the screen.

6. Type **R** twice to return to the Main Menu. Type **S** to select Save Configuration Changes.

Your changes are saved. The port mirror is now functional.

Modifying a Source Port Mirror

Use the following procedure to add, delete, set (overwrite), or clear a source port mirror. For information about how to specify a port, see **Specifying Ports** on page 26. To save your changes, return to the Main Menu and select **S** - Save Configuration Changes.

To modify a source port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 22 on page 77.
2. From the Port Menu, type **6** to select Port Mirroring.
The Port Mirroring menu in Figure 32 on page 109 is displayed.
3. Type **2** to select Modify Mirror.
The following menu is displayed.

```

Allied Telesyn AT-8400 Series - AT-S60
High School Switch

Login Privilege: Manager

                                Modify Mirror

Destination Mirror Port      Source Mirror Port(s)      Status
-----
3.4                          8.4, 9.6                  Enabled
4.5                          10.1, 11.1, 12.1         Enabled

1 - Add Source Port(s)
2 - Delete Source Port(s)
3 - Set Source Port(s)
4 - Clear Source Port(s)

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

4. Select **1**- Add Source Port(s) to add a source port mirror to a current list.

The following prompt appears:

```
Enter Destination Port:
```

5. Enter the destination mirror port from the list at the top of the menu and press Return.

For information about how to specify a port, see **Specifying Ports** on page 26.

The following prompt appears:

Enter Source Port(s) [port-list]:

6. Enter the source mirror port (s) or port list and press Return.

Note

You cannot assign a range of ports as source mirror ports.

The display at the top of the Port Mirroring menu is updated.

7. To delete a source port mirror, enter **2**.

The following prompt appears:

Enter Destination Port:

8. Enter the destination port from the list at the top of the screen and press Return.

The following prompt appears:

Enter Source Port(s) [port-list]:

9. Enter the source mirror port(s) or port list and press Return.

The source and destination mirror ports are removed from the display at the top of the menu.

10. To set, or overwrite, a source mirror port, enter **3**.

The following prompt appears:

Enter Destination Port:

11. Enter the destination port from the list at the top of the screen and press Return.

The following prompt appears:

Enter Source Port(s) [port-list]:

12. Enter the new source mirror port(s) or port list and press Return.

13. To clear, or remove, all source mirror ports from a port mirror, type **4**.

The following prompt appears:

Enter Destination Port:

14. Enter the destination mirror port from the list at the top of the screen and press Return.

All source mirror ports are removed from the Modify Mirror Menu.

15. Type **R** twice to return to the Main Menu. **S** to select Save Configuration Changes.

The port mirror is updated with your changes.

Deleting a Destination Port Mirror

To delete a destination port mirror and its source mirror port(s), perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **6** to select Port Mirroring.

The Port Mirroring menu in Figure 32 on page 109 is displayed.

3. Type **3** to select Delete Mirror.

The following prompt is displayed.

Enter Destination Port:

4. Enter the destination mirror port from the list at the top of the menu and press Return.

For information about how to specify a port, see **Specifying Ports** on page 26.

The destination port and the source port(s) are removed from the display at the top of the Port Mirroring menu.

5. Type **R** twice to return to the Main Menu. Type **S** to select Save Configuration Changes.

The port mirror on the switch is deleted. The port that was functioning as the port mirror is now available for normal network operations.

Enabling a Destination Port Mirror

Use this procedure if you have previously disabled a destination port mirror (see **Disabling a Destination Port Mirror** on page 115) and you want to make it active again.

To enable a destination port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **6** to select Port Mirroring.

The Port Mirroring menu in Figure 32 on page 109 is displayed.

3. Type **4** to select Enable Mirror.

The following prompt is displayed.

```
Enter Destination Port [port-list, all]:
```

4. Enter the mirror port that you want to enable and press Return.

port-list

For information about how to specify ports, see **Specifying Ports** on page 26.

all

Use this selection to enable all the mirror ports listed on the Port Mirroring Menu.

At the top of the Port Mirroring menu, the Status column changes to Enabled.

Note

By default, the mirror is enabled when it is created.

5. Type **R** twice to return to the Main Menu. Type **S** to select Save Configuration Changes.

The port mirror (or port mirrors) is now enabled.

Disabling a Destination Port Mirror

Use this procedure to prevent traffic from the source mirror port from being mirrored to the destination port. You may want to use this procedure to temporarily stop mirroring the source traffic while reserving the destination port for mirroring.

To disable a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **6** to select Port Mirroring.
The Port Mirroring menu in Figure 32 on page 109 is displayed.
3. Type **5** to select Disable Mirror.

The following prompt is displayed.

Enter Destination Port [port-list, all]:

4. Enter the mirror port that you want to disable and press Return.

port-list

For information about how to specify ports, see **Specifying Ports** on page 26.

all

Use this selection to disable all the mirror ports listed on the Port Mirroring Menu.

At the top of the Port Mirroring menu, the Status column changes to Disabled.

5. Type **R** twice to return to the Main Menu. Type **S** to select Save Configuration Changes.

The port mirror is now disabled.

Chapter 9

STP, RSTP, and MSTP

This chapter provides background information on the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). The chapter also contains procedures on how to adjust spanning tree bridge and port parameters. The sections in this chapter include:

- ❑ **STP and RSTP Overview** on page 117
- ❑ **Enabling or Disabling STP, RSTP, or MSTP** on page 128
- ❑ **Configuring STP** on page 130
- ❑ **Configuring RSTP** on page 135
- ❑ **MSTP Overview** on page 141
- ❑ **Configuring MSTP** on page 156

Note

For further information on Spanning Tree Protocol, refer to IEEE Std 802.1d. For further information on Rapid Spanning Tree Protocol, refer to IEEE Std 802.1w. For further information on Multiple Spanning Tree Protocol, refer to IEEE Std 802.1s.

STP and RSTP Overview

A physical loop in a network topology can pose a significant problem to Ethernet network performance. A loop exists when two or more nodes on a network can transmit data to each other over more than one data link. The problem with physical loops is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and significantly reduce network performance.

STP and RSTP prevent data loops from forming by ensuring that only one path exists between the end nodes in your network. Should one of the protocols detect multiple paths, it places the extra paths in a standby or blocking mode, leaving only one main active path.

STP and RSTP can also activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

The principal difference between the two protocols is in the time each takes to complete the process commonly referred to as *convergence*. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain intercommunications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute to complete in a large network. This can result in lost data packets and the loss of intercommunication between various parts of the network during the convergence process.

RSTP is much faster. It can complete a convergence in seconds, and so diminish the possible impact the process can have on your network.

The STP implementation on the AT-8400 Series switch complies with the IEEE 802.1d standard. The RSTP implementation complies with the IEEE 802.1w standard. The following subsections provide a basic overview on how STP and RSTP operate and define the different parameters that you can adjust.

Note

Spanning tree is disabled by default on the switch.

Note

An AT-8411 line card with more than four ports functioning as redundant links to other network devices can significantly retard the speed of convergence for STP and RSTP. You can avoid this problem by selecting ports on different line cards to function as redundant links.

**Bridge Priority
and the Root
Bridge**

The first task that bridges perform when a spanning tree protocol is activated on a network is the selection of a *root bridge*. A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by a combination of a *bridge priority* number, also referred to as the bridge identifier, and sometimes the bridge's MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

The bridge priority number can be changed on an AT-8400 Series switch. You can designate which switch on your network you want as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge off-line, and assign that bridge the second lowest bridge identifier number.

The range for STP and RSTP bridge priority is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments. You set the parameter by specifying the increment that represents the desired bridge priority value. Table 1 lists the bridge priority value increments. As an example, if you wanted to set a bridge priority value on a switch to 45056, you would select increment 11. The default value is 32,768, increment 8.

Table 1 Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Path Costs and Port Costs

Once the Root Bridge has been selected, the bridges must determine if the network contains redundant paths and, if one is found, they must select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge* and the port through which the bridge is communicating with the root bridge is referred to as the *root port*.

If redundant paths exist, the bridges that are a part of the paths must determine which path will be the primary, active path, and which path(s) will be placed in the standby, blocking mode. This is accomplished by an determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into blocking state.

Path cost is determined through an evaluation of *port costs*. Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is simply the cumulation of the port costs between a bridge and the root bridge.

The port costs of the ports on an AT-8400 Series switch can be adjusted through the management software. For STP, the range is 0 to 65,535. For RSTP, the range is 0 to 200,000,000.

The default value of 0 activates auto-detection. This feature sets port cost according to port speed, assigning lower costs to ports operating at higher speeds.

The auto-detection default speeds differ for STP and RSTP. Table 2 lists the auto-detection default values for STP.

Table 2 STP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	100
100 Mbps	10
1000 Mbps	4

Table 3 lists the auto-detection default values for RSTP.

Table 3 RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2000000
100 Mbps	200000
1000 Mbps	20000

You can override Auto-Detect and set the port cost manually.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter. This parameter can be used as a tie-breaker when two paths have the same cost.

The range for port priority is 0 to 240 in increments of 16. Just as with the bridge priority value, you specify the increment that corresponds to the desired value. Table 4 lists the port priority increments. The default value is 128, with an increment of 8.

Table 4 Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Forwarding Delay and Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology may also change. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It might take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporarily data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states, listening and learning, before it begins to forward frames. The amount of time a port spends in these states is set by the *forwarding delay* value. This value controls the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable on the AT-8400 Series switch through the management software. The appropriate value for this parameter will depend on a number of variables, with the size of your network being a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is unnecessarily delayed, which could result in the delay or loss of some data packets.

Note

The forwarding delay parameter applies only to STP.

Hello Time and Bridge Packet Data Units (BPDU)

The bridges in a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the Bridge Packet Data Unit (BPDU). When a bridge is brought on-line, it will issue a BPDU in order to determine whether a root bridge has already been selected on the network. and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge will periodically transmit a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *Hello Time*. This is a value that you can set on the AT-8400 Series switch. The interval is measured in seconds and the default is 2 seconds. Consequently, if an AT-8400 Series switch is selected as the Root Bridge of a spanning tree domain, it will transmit a BPDU every two seconds.

Point-to-Point Ports and Edge Ports

Note

This section applies only to RSTP.

Part of the task of configuring RSTP is defining the port types on the bridge. This relates to the device(s) connected to the port. With port type defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections:

- ☐ Point-to-point
- ☐ Edge port

If a bridge port is operating in full-duplex mode, then the port is functioning as point-to-point. Figure 33 illustrates an AT-8400 chassis and an AT-8024 switch that have been interconnected with one data link. With the link operating in full-duplex, the ports are said to be point-to-point ports.

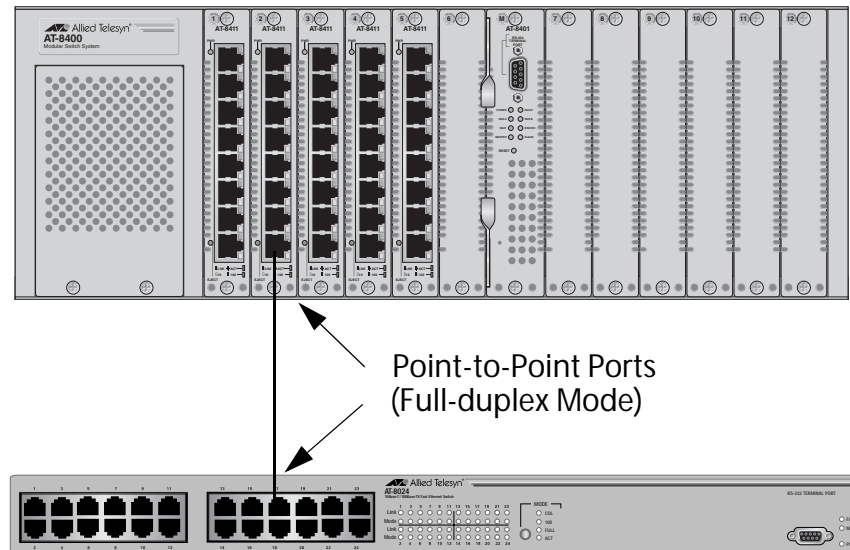


Figure 33 Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then the port is an edge port. Figure 34 illustrates an edge port on an AT-8411 line card in an AT-8400 chassis. The port is connected to an Ethernet hub, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is connected to a device operating at half-duplex mode and there are no participating STP or RSTP devices connected to it.

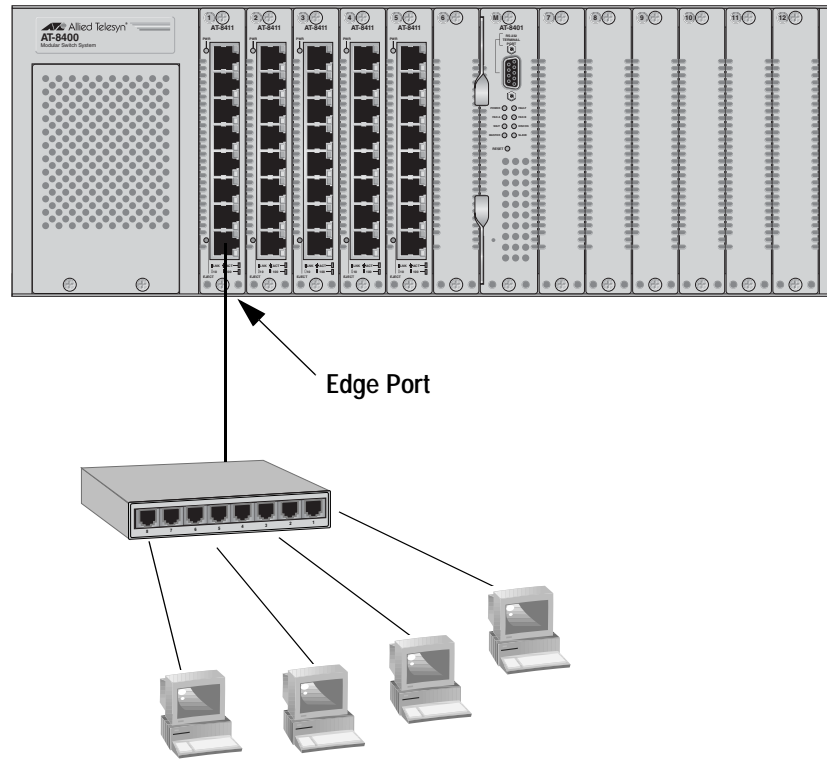


Figure 34 Edge Port

A port can be both point-to-point and edge at the same time. It would operate in full-duplex and have no STP or RSTP devices connected to it. Figure 35 illustrates a port on an AT-8411 line card functioning both as point-to-point and edge.

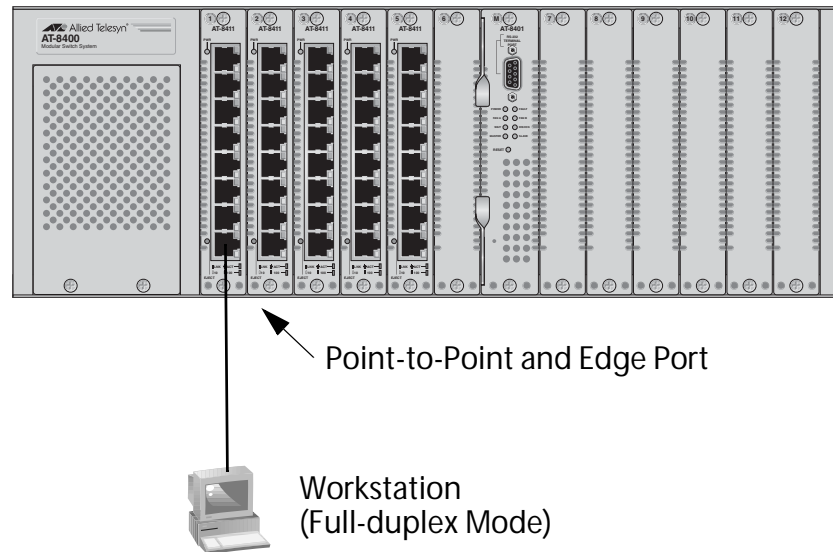


Figure 35 Point-to-Point and Edge Point

Determining whether a bridge port is point-to-point, edge, or both, can be a bit confusing. For that reason it might be best not to change the default values for this RSTP feature unless you have a good grasp of the concept. In most cases, the default values will work fine.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. Your network can consist of bridges running both protocols. STP and RSTP in the same network should be able to operate together to create a single spanning tree domain.

There is no reason not to activate RSTP on an AT-8400 Series switch even when all other switches are running STP. The AT-8400 Series switch can combine its RSTP with the STP of the other switches. An AT-8400 Series switch will monitor the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets will operate in RSTP while ports receiving STP BPDU packets will operate in STP.

Spanning Tree and VLANs

The STP and RSTP implementations on an AT-8400 Series switch are single-instance spanning trees. They support one spanning tree domain. (To define multiple spanning trees, you can use MSTP. For information, refer to **MSTP Overview** on page 141.)

The single spanning tree encompasses all ports on the switch. If the ports are grouped into different VLANs, the spanning tree crosses the VLAN boundaries. This can pose a problem where multiple VLANs that span different switches are connected with untagged ports. What can occur is that spanning tree will block a data link because it detects a physical data loop. This can cause fragmentation of your VLANs.

This is illustrated in Figure 36. Two VLANs, Sales and Production, span one AT-8400 Series switch and one AT-8024GB switch. Two links consisting of untagged ports interconnect the separate parts of each VLAN. If spanning tree is activated on the switches, one of the links would be disabled because spanning tree, which crosses the VLAN boundaries, would see the links as forming a physical loop, even though the VLAN traffic itself does not cross the boundaries.

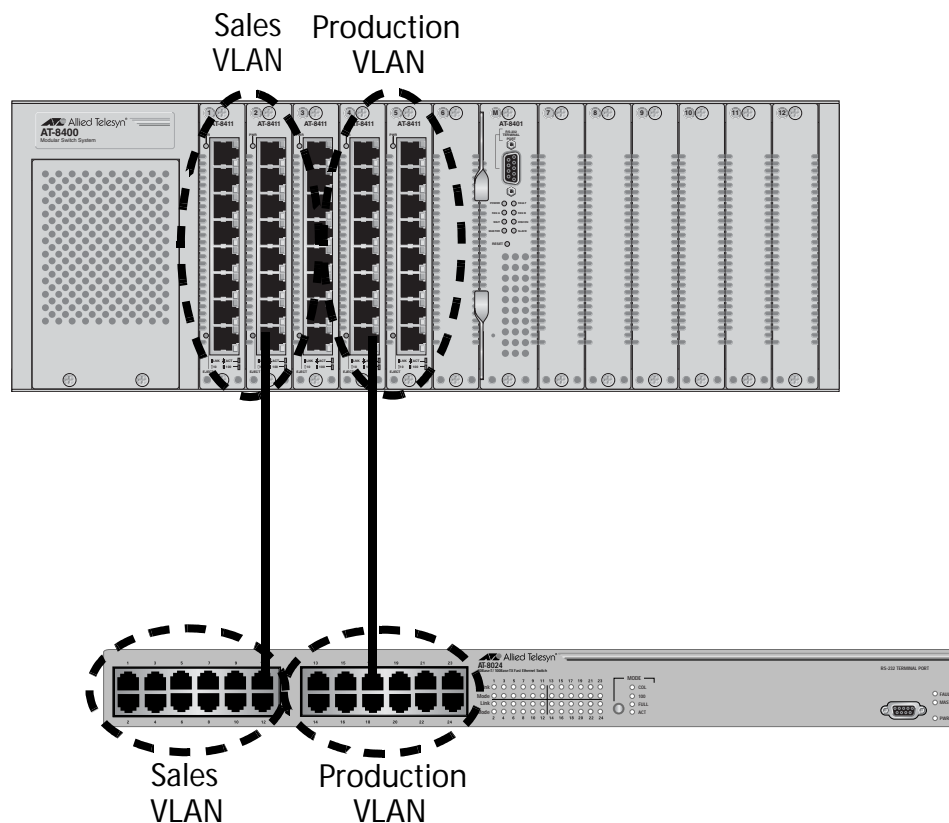


Figure 36 VLAN Fragmentation

There are several approaches that you can take to resolve this problem. One is not to activate STP or RSTP on your network. This solution mandates vigilance on your part not to create network loops when wiring your network.

Another approach is to connect your VLANs with tagged ports instead of untagged ports. A tagged port can handle traffic from more than one VLAN at a time. For information on tagged and untagged ports, refer to **Chapter 10, Virtual LANs** on page 168.

You can also place different VLANs in different spanning trees. This is accomplished using the Multiple Spanning Tree Protocol, explained in **MSTP Overview** on page 141.

Enabling or Disabling STP, RSTP, or MSTP

The AT-8400 Series switch can support STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. So before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol on the switch. Once you have selected it as the active protocol, you can then enable or disable it.

To select the active spanning tree protocol and to enable or disable it, perform the following procedure:

Note

Changing the active spanning tree protocol resets the switch.

1. From the Main Menu, type **3** to select Spanning Tree Menu.

The Spanning Tree Menu in Figure 37 is displayed.

```

Allied Telesyn AT-8400 Series AT-S60
Login Privilege: Manager

          Spanning Tree Menu

1 - Spanning Tree Status ..... Disabled
2 - Active Protocol Version ... RSTP
3 - STP Configuration
4 - RSTP Configuration
5 - MSTP Configuration

R - Return to Previous Menu

Enter your selection?
```

Figure 37 Spanning Tree Menu

Note

If you do not want to change the active spanning tree protocol and just want to enable or disable it, go to step 6.

2. To change the active version of spanning tree protocol on the switch, type **2** to select Active Protocol Version.

The following prompt is displayed:

```

This operation will need a reboot of the system.
Do you want to continue [Y/N] ->
```

3. Type **Y** for yes.

The following prompt is displayed:

Enter new value (S-STP, R-RSTP, M-MSTP) :

4. Type **S** to select STP, **R** to select RSTP, or **M** to select MSTP.

The following prompt is displayed:

Do you want to enable spanning tree? (Y/N) ->

If you respond with Yes to this prompt, the management software reboots the switch and enables the selected spanning tree protocol. If you respond with No, the management software reboots but does not activate spanning tree. The first response is appropriate if you do not want to configure the spanning tree parameter settings before spanning tree is activated. A response of No is appropriate if you want to configure spanning tree parameters before spanning tree is activated.

5. Type **Y** for yes or **N** for no.

The switch reboots and the selected spanning tree protocol becomes the active protocol on the switch. You can now configure the parameters of the selected spanning tree protocol. If you selected STP, go to **Configuring STP** on page 130 for further instructions. If you selected RSTP, go to **Configuring RSTP** on page 135. If you selected MSTP, go to **MSTP Overview** on page 141.

Unlike other management procedures with the AT-S60 software, this procedure does not require you to return to the Main Menu to save your changes. The change to the active spanning tree protocol is automatically saved before the switch reboots.

Note

Steps 6, 7, and 8 apply only if you did not enable the spanning tree when you selected it. The steps enable or disable the spanning tree protocol.

6. To enable or disable the active spanning tree, type **1** to select Spanning Tree Status.
7. Type **E** to enable spanning tree or **D** to disable it. The default is enabled.
8. Return to the Main Menu and type **S** to save your changes.

Configuring STP

This section contains the following procedures:

- ❑ **Configuring STP Bridge Settings** on page 130
- ❑ **Configuring STP Port Settings** on page 132

Configuring STP Bridge Settings

This section contains the procedure for configuring a bridge's STP settings.



Caution

The default STP parameters are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

Note

You cannot configure the STP settings unless the protocol has been selected as the active spanning tree protocol on the switch. For instructions, refer to **Enabling or Disabling STP, RSTP, or MSTP** on page 128.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is displayed in Figure 37 on page 128.
2. From the Spanning Tree Menu, type **3** to select STP Configuration.

The STP Menu is displayed in Figure 38.

```

Allied Telesyn AT-8400 Series AT-S60
Login Privilege: Manager

                        STP Menu

1 - Bridge Priority ..... 32768
2 - Bridge Hello Time ... 2
3 - Bridge Forwarding ... 15
4 - Bridge Max Age ..... 20
5 - Bridge Identifier ... 00:30:84:EE:31:01

P - STP Port Parameters
R - Reset STP to Defaults

R - Return to Previous Menu

Enter your selection?:

```

Figure 38 STP Menu

3. Adjust the bridge STP settings as needed. The parameters are described below.

1 - Bridge Priority

The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from **0** (zero) to **61,440** in increments of 4096, with **0** being the highest priority. For a list of the increments, refer to **Table 1, Bridge Priority Value Increments** on page 119.

2 - Bridge Hello Time

The time interval in seconds between generating and sending configuration messages by the bridge. This parameter can be from **1 to 10** seconds. The default is **2** seconds.

3 - Bridge Forwarding

The waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is **15** seconds.

4 - Bridge Max Age

The length of time in seconds after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default **20**, all bridges delete current configuration messages after **20** seconds. This parameter can be from **6 to 40** seconds. The default is **20** seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be less then $(2 \times (\text{HelloTime} + 1))$.

MaxAge must be less then $(2 \times (\text{ForwardingDelay} - 1))$.

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

5 - Bridge Identifier

The MAC address of the AT-8401 management card. This is used as a tie breaker if two bridges have the same bridge priority number. You cannot change this value.

4. To change STP port settings, go to the next procedure. If you do not want to change STP port settings, return to the Main Menu and type **S** to select Save Configuration Changes.

Configuring STP Port Settings

To adjust a port's STP parameters, perform the following procedure:

1. From the Spanning Tree Menu, type **3** to select STP Configuration.
2. From the STP Menu, type **P** to select STP Port Parameters.

The STP Port Parameters Menu is displayed in Figure 39.

```

Allied Telesyn AT-8400 Series AT-S60
Login Privilege: Manager

                STP Port Parameters

1 - Configure STP Port Settings
2 - Display STP Port Configuration

R - Return to Previous Menu

Enter your selection?
```

Figure 39 STP Port Parameters Menu

3. Type **1** to select Configure STP Port Settings.

The following prompt is displayed:

Enter port-list:

4. Enter the port to configure. For instance, to configure Port 8 on the line card in slot 2, you would enter "2.8". You can configure more than one port at a time. For instructions on how to specify port numbers, refer to **Specifying Ports** on page 26.

The STP Port Configuration menu is displayed in Figure 40.

```

Allied Telesyn AT-8400 Series AT-S60
Login Privilege: Manager

          Configure STP Port Settings
Configuring Ports 1.4
1 - Port Priority ..... 128
2 - Port Cost ..... Automatic-Update

R - Return to Previous Menu

Enter your selection?
```

Figure 40 Configure STP Port Settings Menu

5. Adjust the settings as desired. The parameters are described below.

1 - Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to **Table 4, Port Priority Value Increments** on page 121.

2 - Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. If you select Auto-Detect, the management software assigns a value of 100 if the port is operating at 10 Mbps, 10 for 100 Mbps, and 4 for one gigabit.

6. After adjusting the parameters, return to the Main Menu and type **S** to select Save Configuration Changes.

Displaying STP Port Settings

To display port STP settings, perform the following procedure:

1. From the Spanning Tree Menu, type **3** to select STP Configuration.
2. From the STP Menu, type **P** to select STP Port Parameters. The STP Port Parameters Menu is displayed in Figure 39.
3. From the STP Port Parameters Menu, type **2** to select Display STP Port Configuration.

The Display STP Port Configuration window is displayed in Figure 41.

Allied Telesyn AT-8400 Series AT-S60			
Login Privilege: Manager			
Display STP Port Configuration			
Port	State	Cost	Priority

1.1	Disabled	Auto-Update	128
1.2	Disabled	Auto-Update	128
1.3	Disabled	Auto-Update	128
1.4	Disabled	Auto-Update	128
1.5	Disabled	Auto-Update	128
1.6	Disabled	Auto-Update	128
1.7	Disabled	Auto-Update	128
1.8	Disabled	Auto-Update	128
N - Next Page			
U - Update Display			
R - Return to Previous Menu			

Figure 41 Display STP Port Configuration Window

Configuring RSTP

This section contains the following procedures:

- ❑ **Configuring RSTP Bridge Settings** on page 135
- ❑ **Configuring RSTP Port Settings** on page 138

Configuring RSTP Bridge Settings

This section contains the procedure for configuring a bridge's RSTP settings.



Caution

The default RSTP parameters are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

Note

You cannot configure RSTP settings unless the protocol has been selected as the active spanning tree protocol on the switch. For instructions, refer to **Enabling or Disabling STP, RSTP, or MSTP** on page 128.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is displayed in Figure 37 on page 128.
2. From the Spanning Tree Menu, type **4** to select RSTP Configuration.

The RSTP Menu is displayed in Figure 42.

```

Allied Telesyn AT-8400 Series AT-S60
Login Privilege: Manager

                                RSTP Menu

1 - Force Version ..... RSTP
2 - Bridge Priority ..... 32768 <In multiples of 4096: 8>
3 - Bridge Hello Time ... 2
4 - Bridge Forwarding ... 15
5 - Bridge Max Age ..... 20
6 - Bridge Identifier ... 00:30:84:52:11:11

P - RSTP Port Parameters
D - Reset RSTP to Defaults

R - Return to Previous Menu

Enter your selection?

```

Figure 42 RSTP Menu

3. Adjust the parameters as needed. The parameters are defined below.

1 - Force Version

This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode. If you select RSTP, the bridge will operate all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge will operate in RSTP, using the RSTP parameter settings, but it will send only STP BPDU packets out the ports.

2 - Bridge Priority

The priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from **0** (zero) to **61,440** in increments of 4096, with **0** being the highest priority. For a list of the increments, refer to **Table 1, Bridge Priority Value Increments** on page 119.

3 - Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from **1 to 10** seconds. The default is **2** seconds.

4 - Bridge Forwarding

The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is **15** seconds. This setting applies only to ports running in the STP-compatible mode.

5 - Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default **20**, all bridges delete current configuration messages after **20** seconds. This parameter can be from **6 to 40** seconds. The default is **20** seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be less than $(2 \times (\text{HelloTime} + 1))$.

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

6 - Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

4. After adjusting the parameters, return to the Main Menu and type **S** to select Save Configuration Changes.

Configuring RSTP Port Settings

To adjust a port's RSTP parameters, perform the following procedure:

1. From the Spanning Tree Menu, type **4** to select RSTP Configuration.
2. From the RSTP Configuration menu, type **P** to select RSTP Port Parameters.

The following menu is displayed:

```

Allied Telesyn AT-8400 Series AT-S60
Login Privilege: Manager

RSTP Port Parameters

1 - Configure RSTP Port Settings
2 - Display RSTP Port Configuration
3 - Display RSTP Port State

R - Return to Previous Menu

Enter your selection?
```

Figure 43 RSTP Port Parameters Menu

3. Type **1** to select Configure RSTP Port Settings.

The following prompt is displayed:

```
Enter port-list:
```

4. Enter the port to configure. For instance, to configure Port 8 on the line card in slot 2, enter "2.8". You can configure more than one port at a time. For instructions on how to specify port numbers, refer to **Specifying Ports** on page 26. The RSTP Port Configuration menu in Figure 44 is displayed.

```

Allied Telesyn AT-8400 Series AT-S60
Login Session: Manager

          Configure RSTP Port Settings

Configuring Ports 4.8

1 - Port Priority ..... 128
2 - Path Cost ..... Auto Update
3 - Point-to-Point ..... Auto Detect
4 - Edge Port ..... Yes

R - Return to Previous Menu

Enter your selection?

```

Figure 44 Configure RSTP Port Settings Menu

5. Adjust the settings as needed. The parameters are explained below.

1 - Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to **Table 4, Port Priority Value Increments** on page 121.

2 - Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

3 - Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

4 - Edge Port

This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

6. After making your changes, return to the Main Menu and type **S** to select Save Configuration Changes.

Displaying Port RSTP Status

The RSTP Port Parameters menu has two selections for displaying a variety of RSTP port information. The two menu selections are discussed below.

2 - Display RSTP Port Configuration

This selection displays a window that contains the current port settings for the following RSTP parameters:

- ☐ Edge-Port
- ☐ Point-to-Point Port
- ☐ Port Cost
- ☐ Port Priority

3 - Display RSTP Port State

This selection displays a window that contains the following RSTP operating status for a port:

- ☐ State - Identifies the RSTP state of the port. Possible states are: discarding, learning, and forwarding. A state of disabled means the port has not established a link with its end node.
- ☐ Role - Indicates the RSTP role of the port. Possible roles are: root, alternate, backup, and designated.
- ☐ Port Cost - Indicates the port cost of the port.
- ☐ Version - Indicates whether the port is operating in RSTP mode or STP-compatible mode.

MSTP Overview

As mentioned in earlier sections in this chapter, STP and RSTP are referred to as single-instance spanning trees that search for physical loops across all VLANs in a bridged network. When loops are detected, the protocols stop the loops by placing one or more bridge ports in a blocking state.

As explained in **Spanning Tree and VLANs** on page 125, STP and RSTP can result in VLAN fragmentation where VLANs that span multiple bridges are connected together with untagged ports. The untagged ports creating the links can represent a physical loop in the network, which will be blocked by spanning tree. The result can be a loss of communication between different parts of the same VLAN.

One way to resolve this, other than by not activating spanning tree on your network, is to link the switches using tagged ports, which can handle traffic from multiple VLANs simultaneously. The drawback to this approach is that the link formed by the tagged ports can create a bottleneck to your Ethernet traffic, resulting in reduced network performance.

Another approach is to use the Multiple Spanning Tree Protocol (MSTP). This spanning tree shares many of the same characteristics as RSTP. It features rapid convergence and has many of the same parameters. But the main difference is that while RSTP, just like STP, supports only a single-instance spanning tree, MSTP supports multiple spanning trees within a network.

The following sections describe some of the terms and concepts relating to MSTP. If you are not familiar with spanning tree or RSTP, you should first review the section **STP and RSTP Overview** on page 117.

Note

Do not activate MSTP on an AT-8400 Series switch without first familiarizing yourself with the following concepts and guidelines. Unlike STP and RSTP, you cannot activate this spanning tree protocol on a switch without first configuring the protocol parameters.

Multiple Spanning Tree Instance (MTSI)

The individual spanning trees in MSTP are referred to as Multiple Spanning Tree Instances (MSTIs). A MSTI can span any number of AT-8400 Series switches, and an AT-8400 Series switch can support up to 16 MSTIs at a time.

To create a MSTI, you first assign it a number, referred to as the MSTI ID. The range is 1 to 15. (The switch comes with a default MSTI with an MSTI ID of 0. This default spanning tree instance is discussed later in **Common and Internal Spanning Tree (CIST)** on page 149.)

Once you have selected an MSTI ID, you need to define the scope of the MSTI by assigning one or more VLANs to it. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time.

Here are a couple of examples. Figure 45 illustrates two AT-8400 Series switches each containing the two VLANs Sales and Production. The two parts of each VLAN are connected with a direct link using untagged ports on both switches.

If the switches were running STP or RSTP, one of the links would be blocked because the links constitute a physical loop. Which link would be blocked would depend on the STP or RSTP bridge settings. In the example, the link between the two parts of the Production VLAN is blocked, resulting in a loss of communications between the two parts of the Production VLAN.

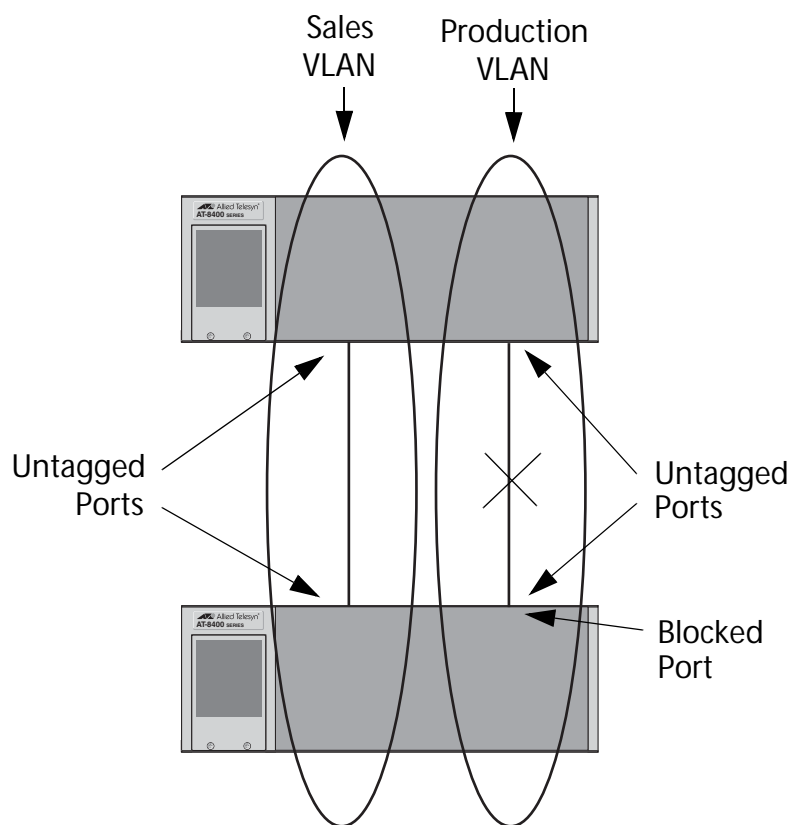


Figure 45 VLAN Fragmentation with STP or RSTP

Figure 46 illustrates the same two AT-8400 Series switches and the same two virtual LANs. But in this example, the two switches are running MSTP and the two VLANs have been assigned different spanning tree instances. Now that they reside in different MSTIs, both links remain active, enabling the VLANs to forward traffic over their respective direct link.

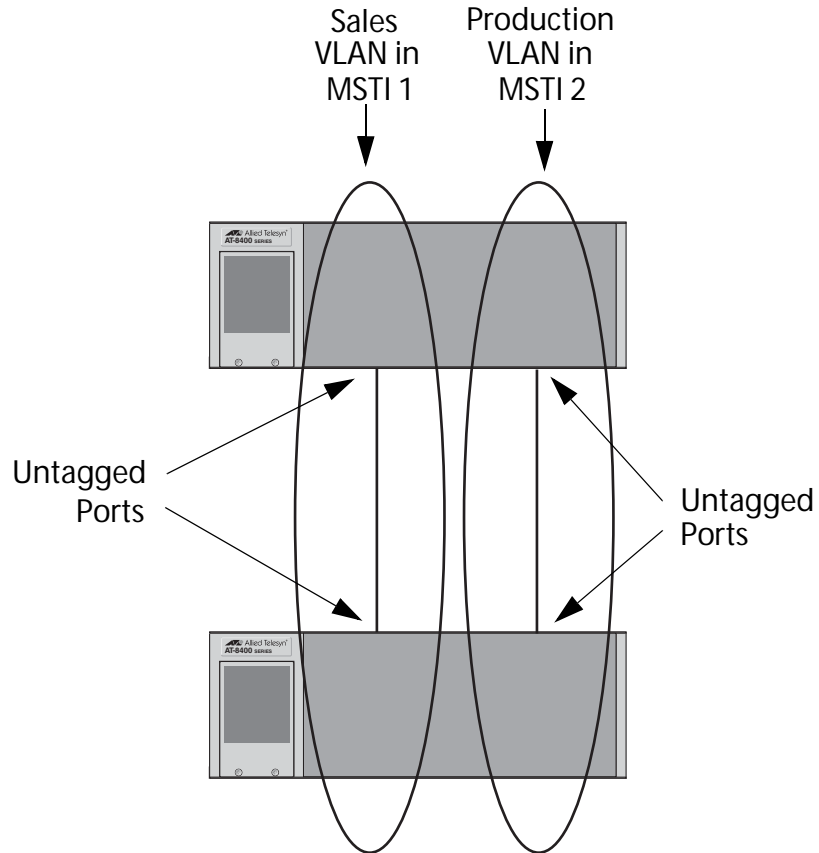


Figure 46 MSTP Example of Two Spanning Tree Instances

A MSTI can contain more than one VLAN. This is illustrated in Figure 47 where there are two AT-8400 Series switches with four VLANs. There are two MSTIs, each containing two VLANs. MSTI 1 contains the Sales and Presales VLANs and MSTI 2 contains the Design and Engineering VLANs.

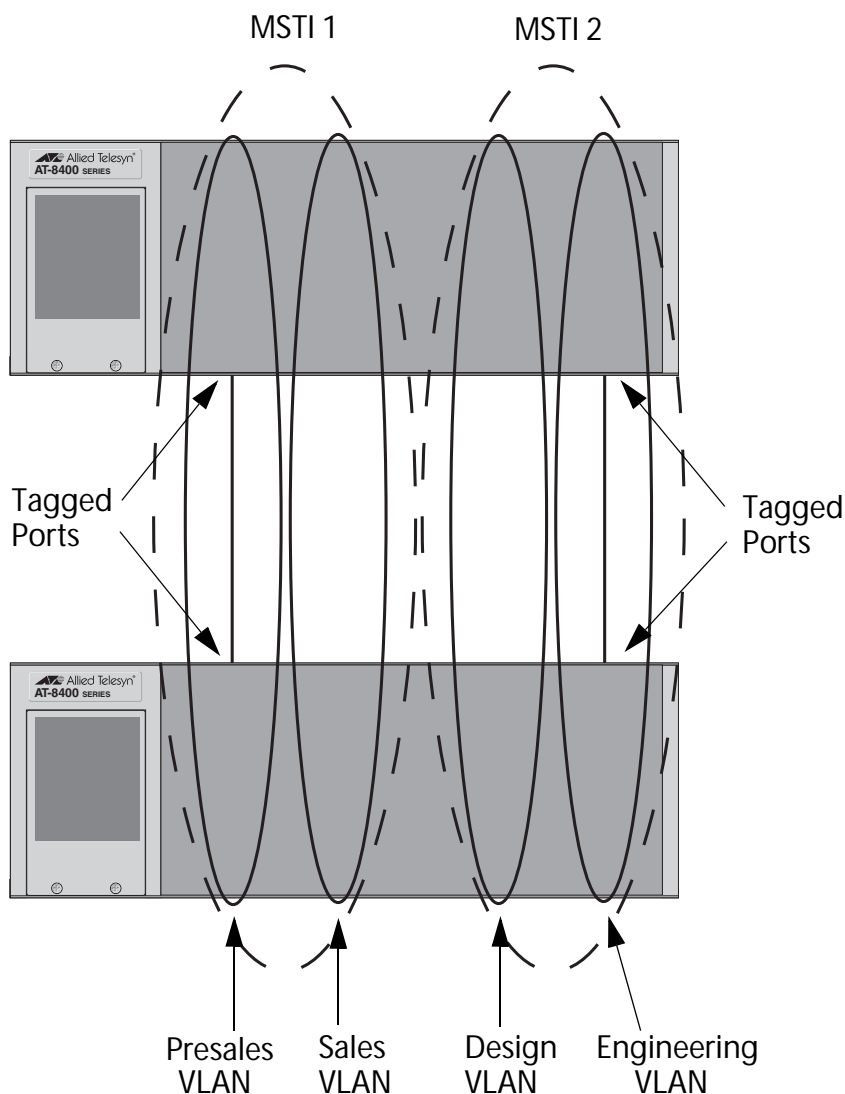


Figure 47 Multiple VLANs in a MSTI

You should note in this example that since an MSTI contains more than one VLAN, the links between the VLAN parts is made with tagged, not untagged, ports so that they can carry traffic from more than one virtual LAN. Referring again to Figure 47, the tagged link in MSTI 1 is carrying traffic for both the Presales and Sales VLANs while the tagged link in MSTI 2 is carrying traffic for the Design and Engineering VLANs.

This example illustrates Allied Telesyn's implementation of MSTP. It shows that a tagged port cannot be a member of VLANs that belong to different MSTIs. That is why each MSTI in the example has its own tagged link.

MSTI Guidelines

Here are a couple guidelines to keep in mind about MSTIs:

- ☐ An AT-8400 Series switch can support up to 16 spanning tree instances, including the CIST, at a time.
- ☐ A MSTI can contain any number of VLANs.
- ☐ A VLAN can belong to only one MSTI at a time.
- ☐ A port on the switch can belong to only one spanning tree instance at a time. This means that a port cannot be a tagged and untagged member of VLANs that belong to different MSTIs. For example, if Port 1 on a line card is an untagged port in one VLAN and a tagged port in three other VLANs, all four VLANs must be assigned to the same MSTI. This rule is required because a port can be either blocking or forwarding; a port cannot perform both functions simultaneously, which could occur if it was a member of VLANs that resided in different spanning tree instances.
- ☐ A router or Layer 3 network device is required to forward traffic between different VLANs.

VLAN and MSTI Associations

Part of the task to configuring MSTP involves assigning VLANs to spanning tree instances. The mapping of VLANs to MSTIs is called *associations*. A VLAN, either port-based or tagged, can belong to only one instance at a time, but an instance can contain any number of VLANs.

Multiple Spanning Tree Regions

Another important concept of MSTP is *regions*. A MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. Those characteristics are:

- ☐ Configuration name
- ☐ Revision number
- ☐ VLANs
- ☐ VLAN to MSTI ID associations

A *configuration name* is a name you assign to a region to help you identify it. You must assign each bridge in a region exactly the same name; even the same upper and lowercase lettering. Identifying the regions in your network is easier if you choose names that are characteristic of the functions of the nodes and bridges of the region. Examples are Sales Region and Engineering Region.

The *revision number* is an arbitrary number you assign to a region. This number can be used to keep track of the revision level of a region's configuration. For example, you might use this value to maintain the number of times you revise a particular MSTP region. It is not important that you maintain this number, only that each bridge in a region have the same number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VIDs must be same on all bridges of a region.

Finally, the VLANs in the bridges must be associated to the same MSTIs.

If any of the above information is different on two bridges, MSTP will consider the bridges as residing in different regions.

Figure 48 is an illustration of the concept of regions. It shows one MSTP region consisting of two AT-8400 Series switches. Each switch in the region has the same configuration name and revision level. The switches also have the same five VLANs and the VLANs are associated with the same MSTIs.

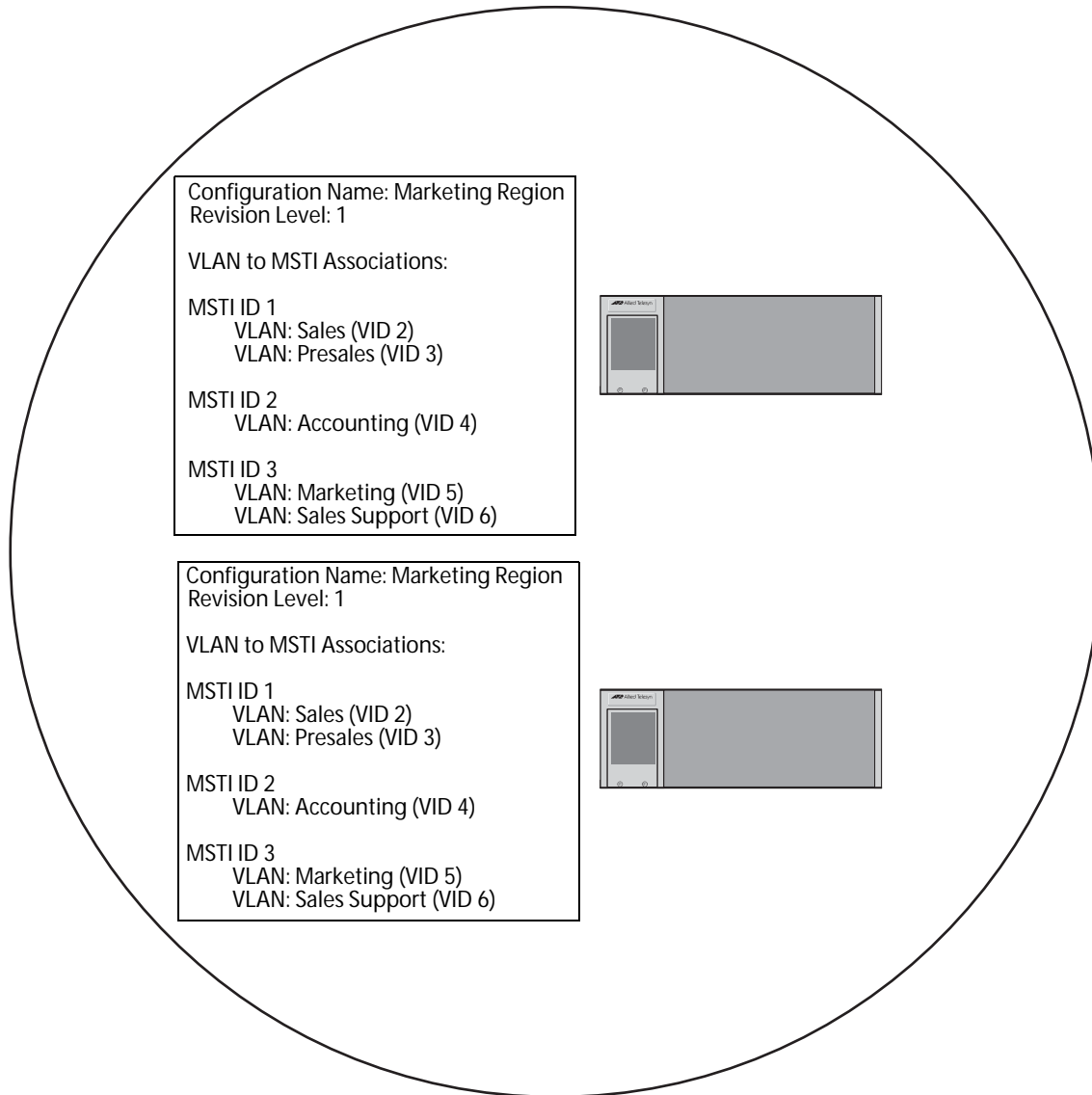


Figure 48 Multiple Spanning Tree Region

The AT-8400 Series switch determines regional boundaries by examining the MSTP BPDUs received on the ports. A port that receives a MSTP BPDU from another bridge with regional information different from its own is considered to be a boundary port and the bridge connected to the port as belonging to another region.

The same is true for any ports connected to bridges running the single-instance spanning tree STP or RSTP. Those ports are also considered as part of another region.

Each MSTI functions as an independent spanning tree within a region. Consequently, each MSTI must have a root bridge to locate physical loops within the spanning tree instance. An MSTI's root bridge is called a *regional root*. The MSTIs within a region may share the same regional root or they can have different regional roots.

A regional root for an MSTI must be within the region where the MSTI is located. An MSTI cannot have a regional root that is outside its region.

A regional root is selected by a combination of the *MSTI priority* value and the bridge's MAC address. The MSTI priority is analogous to the RSTP bridge priority value. Where they differ is that while the RSTP bridge priority is used to determine the root bridge for an entire bridged network, MSTI priority is used only to determine the regional root for a particular MSTI.

The range for this parameter is the same as the RSTP bridge priority; from 0 to 61,440 in sixteen increments of 4,096. To set the parameter, you specify the increment that represents the desired MSTI priority value. Table 1 on page 119 lists the increments.

Region Guidelines

Here are a couple points to remember about regions.

- ☐ A network can contain any number of regions and a region can contain any number of AT-8400 Series switches.
- ☐ An AT-8400 Series switch can belong to only one region at a time.
- ☐ A region can contain any number of VLANs.
- ☐ All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- ☐ An MSTI cannot span multiple regions.

- ❑ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- ❑ The regional root of a MSTI must be in the same region as the MSTI.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTI ID of 0.

This instance has unique features and functions that make it different from the MSTIs that you create yourself. First, you cannot delete this instance and you cannot change its MSTI ID.

Second, when you create a new port-based or tagged VLAN, it is by default associated with the CIST and is automatically given an MSTI ID of 0. The Default_VLAN is also associated by default with CIST.

Another critical difference is that when you assign a VLAN to another MSTI, it still partially remains a member of CIST. This is because CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP single-instance spanning trees in the network. MSTP uses CIST to participate in the creation of a spanning tree between different regions and between regions and single-instance spanning tree, to form one spanning tree for the entire bridged network.

The reason MSTP uses CIST to form the spanning tree of an entire bridged network is because CIST can cross regional boundaries, while a MSTI cannot. If a port is a boundary port, that is, if it is connected to another region, that port automatically belongs solely to CIST, even if it was assigned to an MSTI, because only CIST is active outside of a region.

As mentioned earlier, every MSTI must have a root bridge, referred to as a regional root, in order to locate loops that might exist within the instance. CIST must also have a regional root. However, the CIST regional root communicates with the other MSTP regions and single-instance spanning trees in the bridged network.

The CIST regional root is set with the *CIST Priority* parameter. This parameter, which functions similar to the RSTP bridge priority value, is used to select the root bridge for the entire bridged network. If an AT-8400 Series switch has the lowest CIST Priority value among all the spanning tree bridges, it functions as the root bridge for all the MSTP regions and STP and RSTP single-instance spanning trees in the network.

MSTP with STP and RSTP

MSTP is fully compatible with STP and RSTP. If a port on an AT-8400 Series switch running MSTP receives STP BPDUs, the port sends only STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs since RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered a boundary port of the MSTP region and the bridge as belonging to a different region.

An MSTP region can be considered as a virtual bridge. The implication is that other MSTP regions and STP and RSTP single-instance spanning trees cannot discern the topology or constitution of a MSTP region. The only bridge they will be aware of is the regional root of the CIST instance.

Summary of Guidelines

Careful planning is essential for the successful implementation of MSTP. This section reviews all the rules and guidelines mentioned in earlier sections, and adds a few new ones:

- ☐ An AT-8400 Series switch can support up to 16 spanning tree instances, including the CIST, at a time.
- ☐ A MSTI can contain any number of VLANs.
- ☐ A VLAN can belong to only one MSTI at a time.
- ☐ An MSTI ID can be from 1 to 15.
- ☐ The CIST ID is 0. You cannot change this value.
- ☐ A port on the switch can belong to only one spanning tree instance at a time. This means that a port cannot be a tagged and untagged member of VLANs that belong to different MSTIs. For example, if Port 1 on a line card is an untagged port in one VLAN and a tagged port in three other VLANs, all four VLANs must be assigned to the same MSTI. This rule is required because a port can be either blocking or forwarding; a port cannot perform both functions simultaneously, which could occur if it was a member of VLANs that reside in different spanning tree instances.
- ☐ A router or Layer 3 network device is required to forward traffic between VLANs.
- ☐ A network can contain any number of regions and a region can contain any number of AT-8400 Series switches.
- ☐ An AT-8400 Series switch can belong to only one region at a time.
- ☐ A region can contain any number of VLANs.

- ❑ All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- ❑ An MSTI cannot span multiple regions.
- ❑ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- ❑ The regional root of a MSTI must be in the same region as the MSTI.
- ❑ The CIST must have a regional root for communicating with other regions and single-instance spanning trees.
- ❑ MSTP is compatible with STP and RSTP.
- ❑ A port will transmit CIST information even when it's associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained more in **Associating VLANs to MSTIs** on page 151.)

Note

Due to different vendor implementations of the new IEEE 802.1s standard, compatibility issues concerning MSTP instances between the AT-8400 Series switch and switches from other vendors may exist. This can result in compatibility issues between different MSTP implementations. For this release, MSTP is compatible only with other AT-8400 Series switches.

Associating VLANs to MSTIs

Allied Telesyn recommends that you assign all VLANs on a switch to an MSTI. You should not leave a VLAN assigned to just the CIST, including the Default_VLAN. This is to prevent the blocking of a port that should be in the forwarding state. The reason for this guideline is explained below.

An MSTP BPDU contains the instance to which the port transmitting the packet belongs. By default, all ports belong to the CIST instance. So CIST would be included in the BPDU. If the port is a member of a VLAN that has been assigned to another MSTI, that information is also included in the BPDU.

This is illustrated in Figure 49. Port 8 on a line card in Switch A is a member of a VLAN assigned to MSTI ID 7. Port 1 on another line card in the same switch is a member of a VLAN assigned to MSTI ID 10. The BPDUs transmitted by port 8 to Switch B would indicate that the port is a member of both CIST and MSTI 7, while the BPDUs from Port 1 would indicate the port is a member of the CIST and MSTI 10.

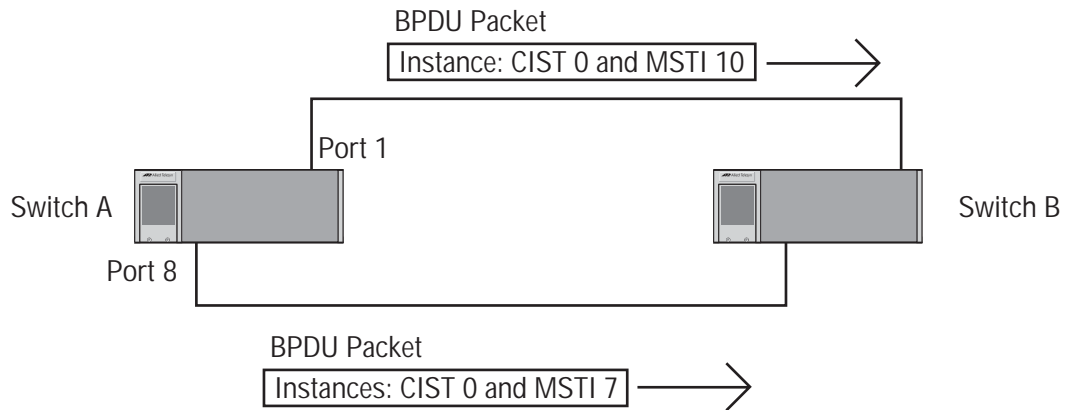


Figure 49 CIST and VLAN Guideline - Example 1

At first glance, it might appear that since both ports belong to CIST, a loop would exist between the switches and that MSTP would block a port to stop the loop. However, within a region, MSTI takes precedence over CIST. When Switch B receives a packet from Switch A, it uses MSTI, not CIST, to determine whether a loop exists. And since both ports on Switch A belong to different MSTIs, Switch B will determine that no loop exists.

Where a problem can arise is if you assign some VLANs to MSTIs while leaving others just to CIST. The problem is illustrated in Figure 50. The network is the same as the previous example. The only difference is that the VLAN containing Port 8 on Switch A has not been assigned to an MSTI, and belongs only to CIST with its MSTI ID 0.

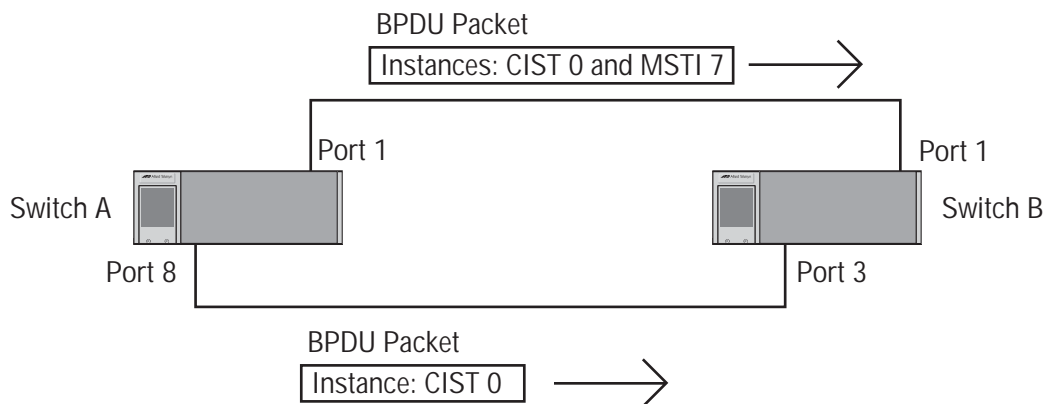


Figure 50 CIST and VLAN Guideline - Example 2

When port 3 on Switch B receives a BPDU, the switch will note the port sending the packet belongs only to CIST. Consequently, Switch B will use CIST in determining whether a loop exists. The result would be that the switch will detect a loop because the other port is also receiving BPDU packets from CIST 0. Switch B would block a port to cancel the loop.

To avoid this issue, always assign all VLANs on a switch, including the Default_VLAN, to an MSTI. This will guarantee that all ports on the switch have an MSTI ID and that will help to ensure that loop detection is based on MSTI, not CIST.

Connecting VLANs Across Different Regions

Special consideration needs to be taken into account when connecting different MSTP regions or an MSTP region and a single-instance STP or RSTP region. Unless planned properly, VLAN fragmentation can occur between the VLANs of your network.

As mentioned previously, only the CIST can span regions. A MSTI cannot. Consequently, you may run into a problem if you use more than one physical data link to connect together various parts of VLANs that reside in bridges in different regions. The result can be a physical loop, which spanning tree will disable by blocking ports.

This is illustrated in Figure 51. The example show two switches, each residing in a different region. Port 1 on a line card in Switch A is a boundary port. It is an untagged member of the Accounting VLAN, which has been associated with MSTI 4. Port 8 on another line card is a tagged and untagged member of three different VLANs, all associated to MSTI 12.

If both switches were a part of the same region, there would be no problem since the ports reside in different spanning tree instances. However, the switches are part of different regions and MSTIs do not cross regions. Consequently, the result would be that spanning tree would determine that a loop exists between the regions, and Switch B would block a port.

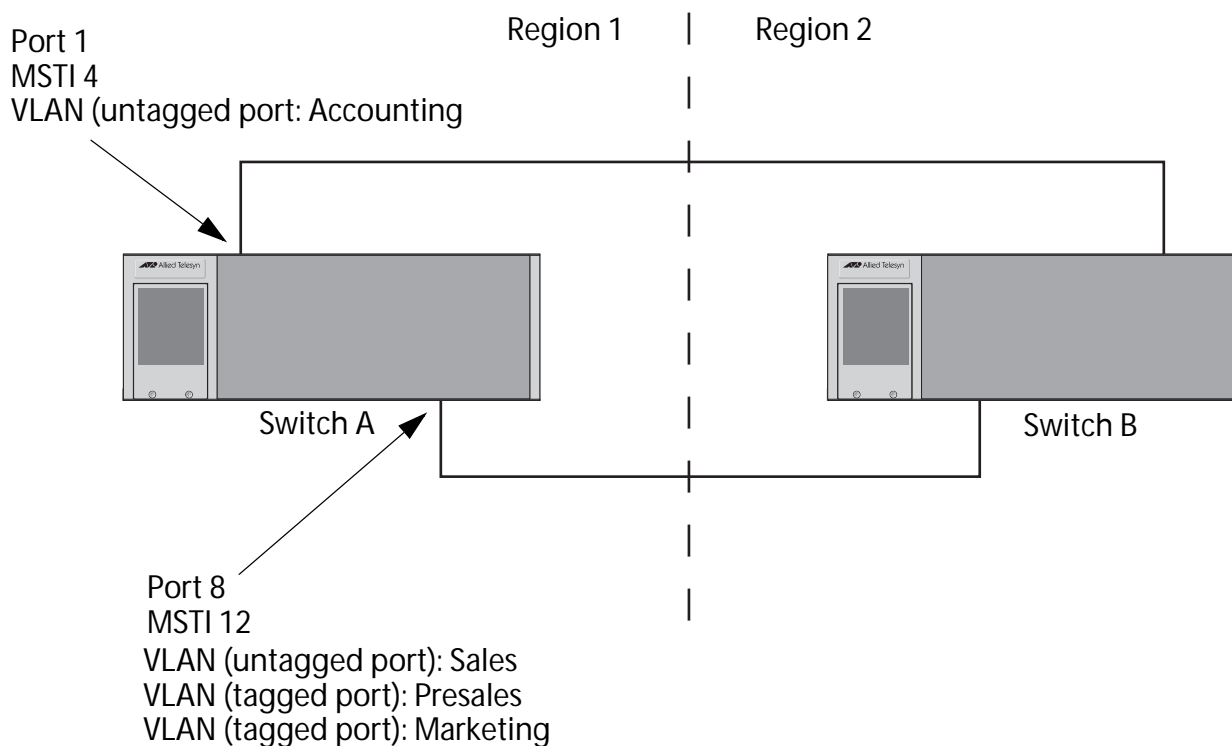


Figure 51 Spanning Regions - Example 1

There are several ways to address this issue. One is to have only one MSTP region for each subnet in your network.

Another approach is to group those VLANs that need to span regions into the same MSTI. Those VLANs that do not span regions can be assigned to other MSTIs.

Here is an example. Let's assume that you have two regions that contain the following VLANs:

Region 1 VLANs

Sales
Presales
Marketing
Advertising
Technical Support
Product Management
Project Management
Accounting

Region 2 VLANs

Hardware Engineering
Software Engineering
Technical Support
Product Management
CAD Development
Accounting

The two regions share three VLANs: Technical Support, Product Management, and Accounting. You could group those VLANs into the same MSTI in each region. For instance, for Region 1 you might group the three VLANs in MSTI 11 and in Region 2 you could group them into MSTI 6. Once grouped, you can connect the VLANs across the regions using a link of tagged ports.

Configuring MSTP

This section contains the following procedures:

- ❑ **Configuring MSTP Bridge Settings** on page 156
- ❑ **Configuring the CIST Priority** on page 159
- ❑ **Creating and Deleting MSTI IDs** on page 160
- ❑ **Associating VLANs to MSTI IDs** on page 162
- ❑ **Configuring MSTP Port Settings** on page 165

Note

You cannot configure MSTP unless the protocol has been selected as the active spanning tree protocol on the switch. For instructions, refer to **Enabling or Disabling STP, RSTP, or MSTP** on page 128.

Configuring MSTP Bridge Settings

This section contains the procedure for configuring a bridge's RSTP settings.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is displayed in Figure 37 on page 128.

2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.

```

Allied Telesyn AT-8400 Series AT-S60
Login Session: Manager

                                MSTP Menu

1 - Force Version ..... MSTP
2 - Hello Time ..... 2
3 - Forwarding Delay ..... 15
4 - Max Age ..... 20
5 - Max Hops ..... 20
6 - Configuration Name .....
7 - Revision Level ..... 0
8 - Bridge Identifier ..... 00:30:24:1E:EE:11

C - CIST Menu
M - MSTI Menu
V - VLAN-MSTI Association Menu
P - MSTP Port Parameters

R - Return to Previous Menu

Enter your selection?

```

Figure 52 MSTP Menu

Menu selections 1 to 8 are described below. Selections C, M, V, and P are described in later sections in this chapter.

3. Adjust the MSTP settings as needed. The selections are described below.

1 - Force Version

This selection determines whether the bridge will operate with MSTP or in an STP-compatible mode. If you select MSTP, the bridge will operate all ports in MSTP, except for those ports that receive STP or RSTP BPDU packets. If you select Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports.

2 - Hello Time

The time interval between generating and sending configuration messages by the bridge. The range of this parameter is 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of the network.

3 - Forwarding Delay

The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

4 - Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs.

All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be less than $(2 \times (\text{HelloTime} + 1))$.

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

5 - Max Hops

MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses an MSTP region boundary. Once the counter reaches zero, the BPDU is deleted.

6 - Configuration Name

The name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters in length. The name, which is case-sensitive, must be the same on all bridges in a region. Examples include Sales Region and Production Region.

7 - Revision Level

The revision level of an MSTP region. The range is 0 (zero) to 255. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision level without conflict.

8 - Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of a root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

4. If you are finished configuring MSTP, return to the Main Menu and type **S** to select Save Configuration Changes.

Configuring the CIST Priority

This procedure explains how to adjust the bridge's CIST priority.

To change the CIST priority, do the following:

1. From the MSTP Menu, type to select **C** to select CIST Menu.

```

Allied Telesyn AT-8400 Series AT-S60
Login Session: Manager

                                CIST Menu

CIST Priority ..... 32768
Associated VLANs ..... 1,2,4,11

1 - Modify CIST Priority

R - Return to Previous Menu

Enter your selection?
```

Figure 53 CIST Menu

The CIST Priority field in the window displays the current value for this MSTP parameter. This number is used in determining the root bridge of the network spanning tree. This number is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

The Associated VLANs field displays the VLAN IDs of the VLANs that are currently associated with CIST and have not been assigned to a MSTI.

2. To change the CIST priority, type **1**.

The following prompt is displayed:

```

Enter new priority [the value will be multiplied by
4096]: [0 to 15] ->
```

- 3. Enter the increment that represents the new CIST priority value. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. For a list of the increments, refer to **Table 1, Bridge Priority Value Increments** on page 119.
- 4. If you are finished configuring MSTP parameters, return to the Main Menu and type **S** to select Save Configuration Changes.

**Creating and
Deleting MSTI
IDs**

This procedure explains how to create and delete MSTI IDs. The procedure also explains how adjust the MSTI priority parameter of a spanning tree instance.

To create or delete an MSTI ID, do the following:

- 1. From the MSTP Menu, type **M** to select MSTI Menu.
The MSTI Menu is shown in Figure 54.

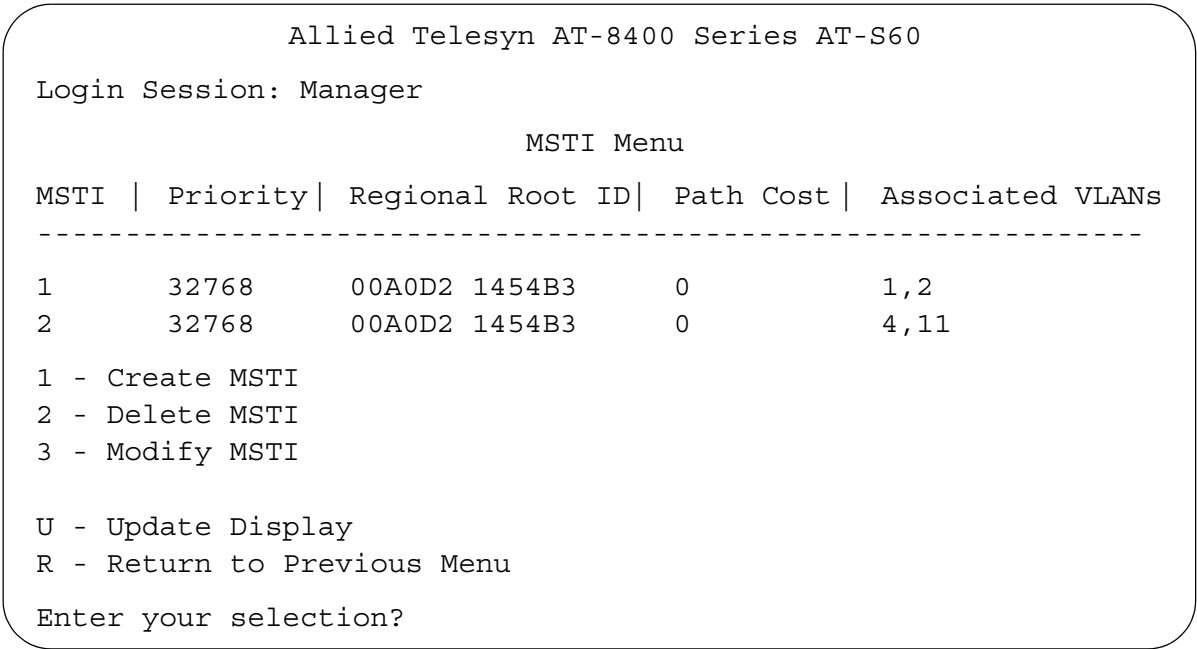


Figure 54 MSTI Menu

The fields in the table are defined below:

MSTI

Lists the MSTI IDs existing on the switch.

Priority

Specifies the MSTI priority value for the MSTI. The steps in this procedure explain how you can assign this value when you create an MSTI ID and how to modify the value for an existing MSTI ID.

Regional Root ID

Identifies the regional root for the MSTI by its MAC address.

Path Cost

Specifies the path cost from the bridge to the regional root. If the bridge is the regional root, the value is 0.

Associated VLANs

Specifies the VIDs of the VLANs that have been associated with the MSTI ID.

The table does not include the CIST. The table will be empty if no MSTI IDs have been created.

2. To create an MSTI ID, do the following:
 - a. Type **1** to select Create MSTI.
The following prompt is displayed:

```
Enter the MSTI ID to be created: [1 to 15] ->
```
 - b. Enter the new MSTP ID. The MSTI IDs range is from 1 to 15. You can specify only one MSTI ID at a time.
The following prompt is displayed:

```
Success...Do you want to associate VLANs with  
this MSTI ID: [Yes/No] ->
```
 - c. If you want to associate VLANs to the MSTI now, type **Y** for yes. If you want to do it later, type **N** for no. (To add or remove VLANs from an existing MSTI, go to **Associating VLANs to MSTI IDs** on page 162.)
If you respond with yes, this prompt appears:

```
Enter the list of VLANs:
```
 - d. Enter the VIDs of the VLANs that you want to associate with the MSTI ID. You can specify more than one VLAN at a time (e.g., 4,6,11) To view VIDs, refer to **Displaying VLANs** on page 185.
3. To delete an MSTI ID, do the following:
 - a. From the MSTI Menu, type **2** to select Delete MSTI.
The following prompt is displayed:

```
Enter the MSTI ID to be deleted: [1 to 15] ->
```
 - b. Enter the MSTP IDs that you want to delete. The range is 1 to 15. (You cannot delete CIST, which has a value of 0.)
All VLANs associated with a deleted MSTP ID are returned to CIST.

4. To change the MSTI priority value for an MSTI, do the following:
 - a. From the MSTI Menu, type **3** to select MSTI Configuration Menu.
The following prompt is displayed:
`Enter the MSTI ID to be modified: [1 to 15] ->`
 - b. Enter the MSTP IDs that you want to modify. The range is 1 to 15.
You can specify only one MSTI ID at a time.
The following prompt is displayed:
`Enter new priority [the value will be multiplied by 4096] [0 to 15] -> 8`
 - c. Enter a new MSTI priority number for this MSTI on the bridge. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. This parameter is used in selecting a regional root for the MSTI. For a list of the increments, refer to **Table 1, Bridge Priority Value Increments** on page 119.
5. If you are finished configuring MSTP parameters, return to the Main Menu and type **S** to select Save Configuration Changes.

Associating VLANs to MSTI IDs

When you create a new MSTI ID, you are given the opportunity of associating VLANs to it. But, once a MSTI ID is created, there might come a time when you want to add more VLANs to it, or perhaps remove VLANs. This procedure explains how to associate VLANs on the switch to an existing MSTI ID and also how to remove VLANs. Before performing this procedure, note the following:

- ☐ You must create a MSTI ID before you can assign VLANs to it. To create a MSTI ID, refer to **Creating and Deleting MSTI IDs** on page 160.
- ☐ You can assign a VLAN to only one MSTI. By default, a VLAN, when created, is associated with the CIST instance, which has a MSTI ID of 0.
- ☐ An MSTI can contain any number of VLANs.

To add or remove a VLAN from an MSTI ID, do the following:

1. From the MSTP Menu, type **V** to select VLAN-MSTI Association Menu.

The VLAN-MSTI Association Menu is shown in Figure 55.

```

Allied Telesyn AT-8400 Series AT-S60
Login Session: Manager

                                VLAN-MSTI Association Menu

MSTI/CIST      Associated VLANs
-----
0
4              1,2
5              6
7              7,22

1 - Add VLANs to MSTI
2 - Delete VLANs from MSTI
3 - Set VLAN to MSTI association
4 - Clear VLAN to MSTI association

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 55 VLAN-MSTI Association Menu

The fields in the table are defined below:

MSTI / CIST

Lists the CIST and current MSTI IDs on the switch.

Associated VLANs

Specifies the VIDs of the VLANs associated with the CIST and MSTI IDs. For instance, referring to the figure above, the VLANs with the VIDs 7 and 22 are assigned to MSTI 7.

2. To associate a VLAN to an MSTP ID, do the following:
 - a. From the VLAN-MSTI Association Menu, type **1** to select Add VLANs to MSTI.

The following prompt is displayed:

```
Enter the MSTI ID <enter 0 for CIST> [0 to 15] ->
```

- b. Enter the MSTI ID to which you want to associate a VLAN.

A prompt similar to the following is displayed:

```
Enter the list of VLANs:
```

- c. Enter the VLAN ID of the virtual LAN you want to associate with the MSTI ID. You can enter more than one VLAN at a time (e.g., 2,4,7). To view VLANs, refer to **Displaying VLANs** on page 185.

The MSTI ID retains any VLANs already associated with it when new VLANs are added.

3. To remove a VLAN to a MSTP ID, do the following:
 - a. From the VLAN-MSTI Association Menu, type **2** to select Delete VLANs from MSTI.

The following prompt is displayed:

```
Enter the MSTI ID <enter 0 for CIST> [0 to 15] ->
```

- b. Enter the MSTI ID to which you want to associate a VLAN.

A prompt similar to the following is displayed:

```
Enter the list of VLANs:
```

- c. Enter the VLAN ID of the virtual LAN that you want to remove from the MSTI ID. You can enter more than one VLAN at a time (e.g., 2,4,7) To view VLANs, refer to **Displaying VLANs** on page 185.

A removed VLAN is returned to CIST.

4. To associate VLANs to an MSTP ID while deleting all VLANs that are already associated with it, do the following:

- a. From the VLAN-MSTI Association Menu, type **1** to select Add VLANs to MSTI.

The following prompt is displayed:

```
Enter the MSTI ID <enter 0 for CIST> [0 to 15] ->
```

- b. Enter the MSTI ID to which you want to associate a VLAN.

A prompt similar to the following is displayed:

```
Enter the list of VLANs:
```

- c. Enter the VLAN ID of the virtual LAN that you want to associate with the MSTI ID. You can enter more than one VLAN at a time (e.g., 2,4,7) (To view VLANs, refer to **Displaying VLANs** on page 185.)

The VLANs already associated with the MSTI ID are removed when the new VLANs are added. The removed VLANs are returned to CIST.

5. If you are finished configuring MSTP, return to the Main Menu and type **S** to select Save Configuration Changes.

Configuring MSTP Port Settings

To adjust a port's MSTP parameters, perform the following procedure:

1. From the MSTP Menu, type **P** to select MSTP Port Parameters.

The MSTP Port Parameters menu is shown in Figure 56.

```

Allied Telesyn AT-8400 Series AT-S60
Login Session: Manager

                MSTP Port Parameters

1 - Configure MSTP Port Settings
2 - Display MSTP Port Configuration
3 - Display MSTP Port State

R - Return to Previous Menu

Enter your selection?

```

Figure 56 MSTP Port Parameters Menu

2. Type **1** to select Configure MSTP Port Settings.

The following prompt is displayed:

Enter port-list:

3. Enter the port to configure. For instance, to configure Port 8 on the line card in slot 2, you would enter "2.8". You can configure more than one port at a time. For instructions on how to specify port numbers, refer to **Specifying Ports** on page 26.

The Configure MSTP Port Settings menu is shown in Figure 57.

```

Allied Telesyn AT-8400 Series AT-S60
Login Session: Manager

                Configure MSTP Port Settings

1 - Port Priority ..... 128
2 - Port Internal Path Cost ..... Auto Update
3 - Port External Path Cost ..... 200000
4 - Point-to-Point ..... Auto Detect
5 - Edge Port ..... Yes

R - Return to Previous Menu

Enter your selection?

```

Figure 57 Configure MSTP Port Settings Menu

4. Adjust the port settings as needed. The selections are described below:

1 - Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value 128). For a list of the increments, refer to **Table 4, Port Priority Value Increments** on page 121.

2- Port Internal Path Cost

The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

3- Port External Path Cost

The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP. The range is 0 to 200,000,000. The default setting is 200,000.

4 - Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

5 - Edge Port

This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

5. If you are finished configuring MSTP parameters, return to the Main Menu and type **S** to select Save Configuration Changes.

Displaying MSTP Port Status

The MSTP Port Parameters menu, shown in Figure 56 on page 165, has two selections for displaying a variety of MSTP port information. The two menu selections are described below. (To display the menu, from the MSTP Menu, type **P** to select MSTP Port Parameters.)

2 - Display MSTP Port Configuration

This selection displays a window that contains the current port settings for the following MSTP parameters:

- ☐ Edge-Port
- ☐ Point-to-Point Port

- ☐ External or Internal Port Cost
- ☐ Port Priority

3 - Display MSTP Port State

This selection displays a window that contains the following MSTP operating status for a port:

- ☐ State - Identifies the MSTP state of the port. Possible states are: discarding, learning, and forwarding. A state of disabled means the port has not established a link with its end node.
- ☐ MSTI-ID - The MSTI ID of the VLAN containing the port. (The MSTI ID for a regional boundary port is always 0, even if the VLAN containing the port has been associated with a MSTI other than CIST.)
- ☐ Role - Indicates the MSTP role of the port. Possible roles are: root, alternate, backup, and designated.
- ☐ Port Cost - The port cost of the port.
- ☐ Version - Indicates whether the port is operating in MSTP mode or STP-compatible mode.

Chapter 10

Virtual LANs

This chapter contains basic information about virtual LANs (VLANs). It also contains the procedures for creating, modifying, and deleting VLANs from a local or Telnet management session. There is also a procedure describing how you can change a switch's VLAN operating mode.

This chapter contains the following sections:

- ❑ **VLAN Overview** on page 169
- ❑ **Port-based VLAN Overview** on page 171
- ❑ **Tagged VLAN Overview** on page 179
- ❑ **Basic VLAN Mode Overview** on page 184
- ❑ **Displaying VLANs** on page 185
- ❑ **Creating a Port-based or Tagged VLAN** on page 187
- ❑ **Example of Creating a Port-based VLAN** on page 191
- ❑ **Example of Creating a Tagged VLAN** on page 192
- ❑ **Modifying a VLAN** on page 193
- ❑ **Deleting a VLAN** on page 196
- ❑ **Setting a Switch's VLAN Mode** on page 197
- ❑ **Specifying a Management VLAN** on page 198

VLAN Overview

A VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. The ports of a VLAN form an independent traffic domain where the unicast, multicast, and broadcast packets generated by the nodes of a VLAN remain within the VLAN.

With VLANs, you can segment your network through the switch's management software and so be able to group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting.

VLANs offer several important benefits:

- ☐ Improved network performance

Network performance often suffers as networks grow in size and as data traffic increases. The more nodes on a LAN segment vying for bandwidth, the more likely overall network performance will decrease.

VLANs improve network performance because VLAN traffic stays within the VLAN. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic not destined for them. It also frees up bandwidth within all the logical workgroups.

- ☐ Increased security

Since traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, VLANs can be used to control the flow of data in your network and prevent data from flowing to unauthorized end nodes.

- ☐ Simplified network management

VLANs can also simplify network management. Before the advent of VLANs, physical changes to the network often had to been made at the switches in the wiring closets. For instance, if an employee changed departments, changing the employee's LAN segment assignment might require a change to the wiring at the switches.

But with VLANs, you can change the LAN segment assignment of an end node connected to the switch through the switch's AT-S60 management software. VLAN memberships can be changed at any time through the management software without moving the

workstations physically, or having to change group memberships by moving cables from one switch port to another.

A virtual LAN can also span more than one switch. This means that the end nodes of a VLAN do not need to be connected to the same switch and so are not restricted to being in the same physical location.

The AT-8400 Series switch supports the following types of VLANs:

- ☐ Port-based VLANs
- ☐ Tagged VLANs

These VLANs are described in the following sections.

Port-based VLAN Overview

As explained in the **VLAN Overview** section, a VLAN consists of a group of ports on one or more Ethernet switches that form an independent traffic domain. The unicast, broadcast, and multicast packets generated by the end nodes of a VLAN remain within the VLAN and do not cross over to the end nodes of other VLANs unless there is an interconnecting device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on a Fast Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. A port-based VLAN also can span switches and consist of ports from multiple Ethernet switches.

Note

All of the Ethernet line cards for the AT-8400 Series switch are pre-configured with one port-based VLAN. All ports are members of this VLAN, called the Default_VLAN.

The parts that make up a port-based VLAN are:

- ☐ VLAN name
- ☐ VLAN Identifier
- ☐ Untagged ports
- ☐ Port VLAN Identifier

VLAN Name

To create a port-based VLAN, you must give it a name. The name should reflect the function of the network devices that are members of the VLAN. Examples include Sales, Production, and Engineering. The names of the VLANs on a switch must be unique. You cannot give two VLANs on the same switch the same name. A VLAN name can be up to 19 alphanumeric characters in length.

VLAN Identifier

Each VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of ports located on one physical switch in your network, you would assign it a VID unique from all other VLANs in your network.

If a VLAN spans multiple switches, then the VID for the VLAN on the different switches must be the same. In this manner, the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches.

For example, if you had a port-based VLAN titled Marketing that spanned three AT-8400 Series switches, you would assign the Marketing VLAN on each switch the same VID.

You can assign this number manually or allow the management software to do it automatically. If you allow the management software to do it automatically, it will simply select the next available VID. This is acceptable when you are creating a new, unique VLAN.

If you are creating a VLAN on a switch that will be part of a larger VLAN that spans several switches, then you will need to assign the number yourself so that the VLAN has the same VID on all switches.

Untagged Ports

Naturally, you need to specify which ports on the switch are to be members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port will not contain any information that indicates VLAN membership, and that VLAN membership will be determined solely by the port's PVID.

A port on a switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be assigned to two port-based VLANs simultaneously.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to the port on which the frame is received, and forwards the frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. Additionally, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, assume that you were creating a port-based VLAN on a switch and you had assigned the VLAN the VID a value of 5. Consequently, the PVID for each port in the VLAN would need to be assigned the value of 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the AT-S60 management software performs this task automatically. The software automatically assigns a PVID to a port, making it identical to the VID of the VLAN to which the port is a member.

General Rules to Creating a Port-based VLAN

Below is a summary of the general rules to observe when creating a port-based VLAN.

- ☐ Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VID.
- ☐ A port can be an untagged member of only one port-based VLAN at a time.
- ☐ The ports on an AT-8400 line card can belong to the same VLAN or to different VLANs.
- ☐ Each port must have a PVID. This value must be the same for all ports in a port-based VLAN and must match a VLAN's VID. This value is assigned automatically by the AT-S60 management software.
- ☐ A port-based VLAN that spans multiple switches requires a dedicated port on each switch to function as an interconnection between the switches where the various parts of the VLAN reside.
- ☐ If end nodes in different VLANs need to communicate with each other, a router or Layer 3 switch is required to interconnect the VLANs.
- ☐ An AT-8400 Series switch can support up to 256 VLANs.

Drawbacks to Port-based VLANs

There are several drawbacks to port-based VLANs:

- ❑ It is not easy to share network resources, such as servers and printers, across multiple VLANs. A router or Layer 3 switch must be added to the network to provide a means for interconnecting the port-based VLANs.
- ❑ The introduction of a router into your network could create security issues from unauthorized access to your network.
- ❑ A VLAN that spans several switches requires a port on each switch for the interconnection of the various parts of the VLAN. For example, a VLAN that spans three switches requires one port on each switch to interconnect the various sections of the VLAN. In network configurations where there are many individual VLANs that span switches, many ports can end up being used ineffectively just to interconnect the various VLANs.

Port-based Examples

What follows are two examples of port-based VLANs that illustrate the basic principles discussed earlier in this chapter.

Example 1

Our first example is illustrated in Figure 58. It shows two port-based VLANs on an AT-8400 switch.

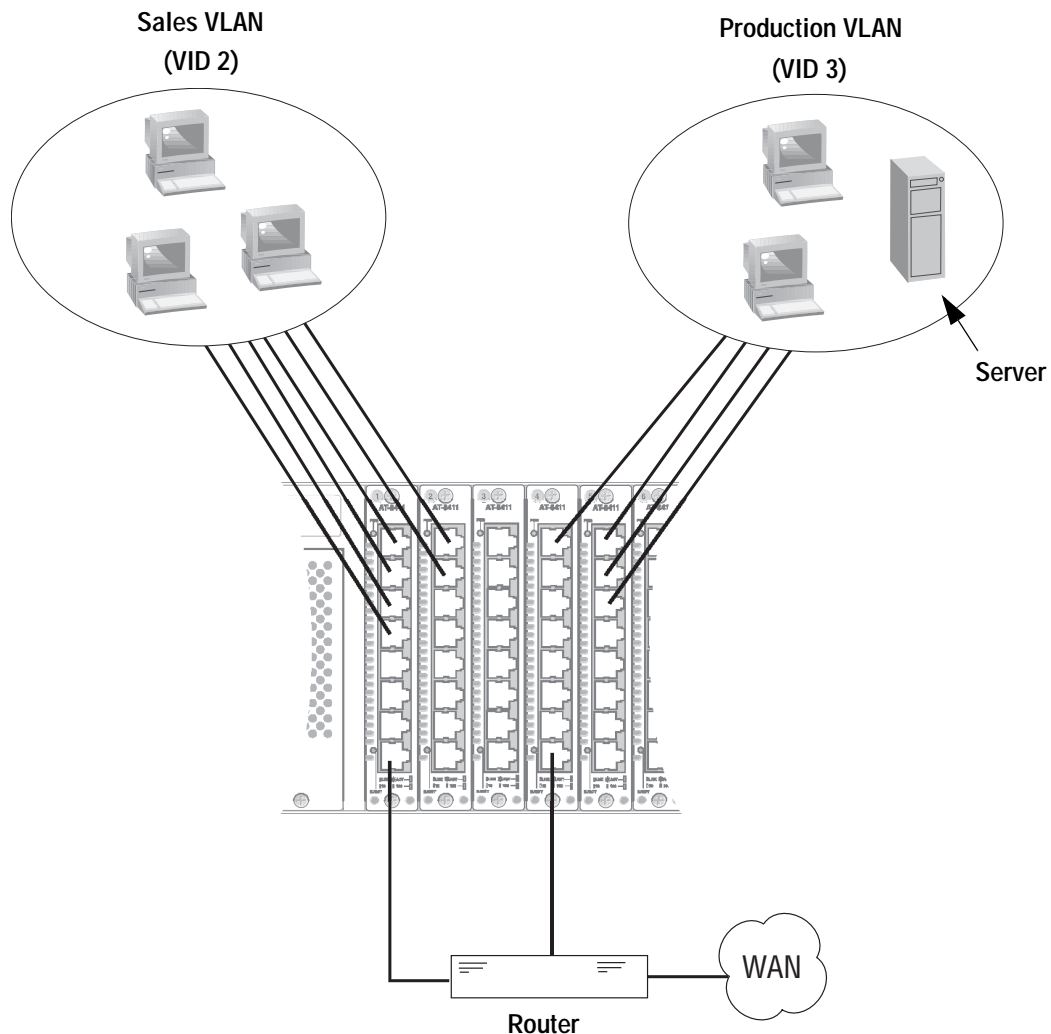


Figure 58 Port-based VLAN - Example 1

The two VLANs are Sales and Production. They were assigned unique VIDs of 2 and 3, respectively, when they were created. (The VID of 1 is reserved for the Default_VLAN.) The ports were also assigned a PVID value that matches the VID of the VLAN in which they were made a member. This is performed automatically by the management software. For instance, all the ports of the Sales VLAN were automatically assigned a PVID of 2 when the ports were made a member of the VLAN.

The table below lists the port assignments for the Sales and Production VLANs on the AT-8400 Series switch.

	Sales VLAN (VID 2)	Production VLAN (VID 3)
AT-8400 Series switch	Slot 1: AT-8411 Ports: 1 - 4, 8 (PVID=2) Slot 2: AT-8411 Ports 1 - 2 (PVID=2)	Slot 4: AT-8411 Ports: 1, 8 (PVID=3) Slot 5: AT-8411 Ports 1 - 3 (PVID=3)

Each VLAN also has a port connected to the router. The router interconnects the VLANs. For instance, if a workstation in the Sales VLAN needs to access the server in the Production VLAN, the traffic passes through the router. Without the router (or a Layer 3 switch), the VLANs could not communicate with each other. The router also provides access for the VLANs to the WAN.

Example 2

Figure 59 illustrates our second port-based example. The two VLANs, Sales and Production, now span two Ethernet switches, an AT-8400 and an AT-8024.

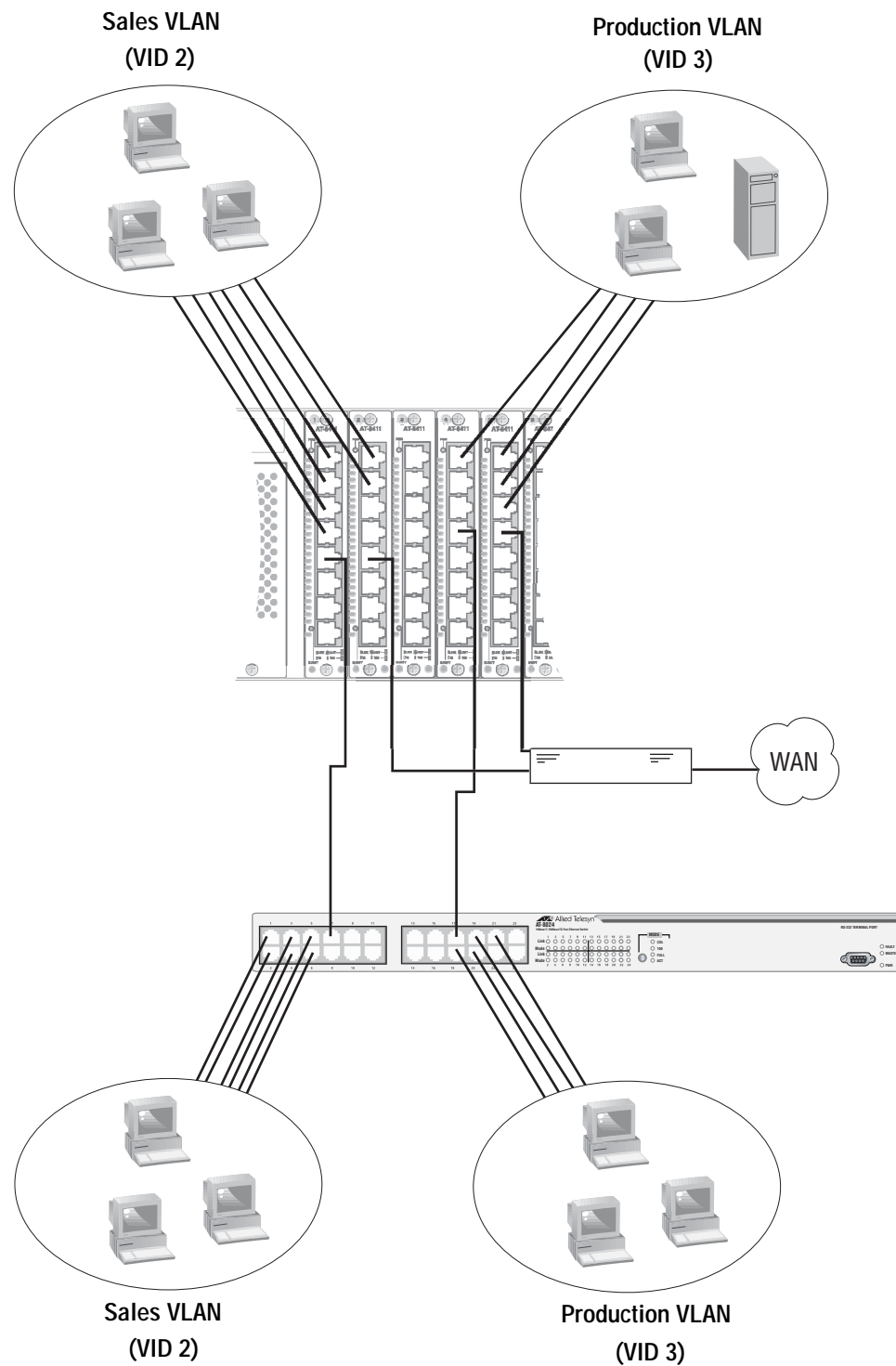


Figure 59 Port-based VLAN - Example 2

The table below lists the port assignments for the Sales and Production VLANs on the switches:

	Sales VLAN (VID 2)	Production VLAN (VID 3)
AT-8400 Series switch	Slot 1 Ports: 1-5 (PVID= 2)	Slot 4 Ports: 1, 4 (PVID= 3)
	Slot 2 Ports: 1-2, 5 (PVID= 2)	Slot 5 Ports: 4 (PVID= 3)
AT-8024 Switch	Ports 1-7 (PVID=2)	Ports 17-21 (PVID= 3)

As mentioned earlier, a VLAN that spans more than one switch requires a data link(s) to connect its different parts together. In our example, both VLANs span multiple switches. So both VLANs need to have a separate link.

For the Sales VLAN, that link is provided by Port 5 on the AT-8411 line card in Slot 1 in the AT-8400 Series switch and by Port 7 in the AT-8024 switch. The connection between the two ports allows the two parts of the Sales VLAN to function as one logical VLAN.

For the Production VLAN, the connection is supplied by Port 4 on the AT-8411 line card in Slot 4 of the AT-8400 Series switch and by Port 17 in the AT-8024 switch.

The two VLANs also need to be connected to the router so they can exchange packets and access the WAN. The Sales VLAN is connected to the router with Port 5 on the AT-8411 line card in Slot 2 of the AT-8400 Series switch. The Production VLAN is connected to the router with Port 4 on the line card in Slot 5.

Tagged VLAN Overview

The second type of VLAN supported by the AT-8400 Series switch is the *tagged VLAN*. Tagged VLANs use information inside the packets themselves as they are received on the ports to determine VLAN membership. This contrasts with port-based VLANs, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). As explained earlier in this chapter in **VLAN Identifier** on page 171, this number uniquely identifies each VLAN in a network.

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

A port to receive or transmit tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of a tagged VLAN is that the tagged ports within the VLAN can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, a server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch for connecting all VLANs on the switch to another switch.

The IEEE 802.1Q standard deals with how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN that the port is a tagged member of, the frame will be accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame will be discarded.

The parts of a tagged VLAN are much the same as those for a port-based VLAN. They are:

- ☐ VLAN Name
- ☐ VLAN Identifier
- ☐ Tagged and Untagged Ports
- ☐ Port VLAN Identifier

Note

For explanations of VLAN name and VLAN identifier, refer back to **VLAN Name** and **VLAN Identifier** on page 171.

Tagged and Untagged Ports

You need to specify which ports will be members of the VLAN. In the case of a tagged VLAN, it will usually be a combination of both untagged ports and tagged ports. You specify which ports will be tagged and which untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs, simultaneously.

Port VLAN Identifier

As explained earlier in the discussion on port-based VLANs, the management software automatically assigns a PVID to each port when a port is made a member of a VLAN. The PVID is always identical to the VLAN's VID, and that in a port-based VLAN packets are forwarded based on the PVID.

Since a tagged port determines VLAN membership by examining the tagged header within the frames that it receives, there would seem to be no need for a PVID. But actually there is. The PVID is used if a tagged port receives an untagged frame (that is, a frame without any tagged information). The port will forward the frame based on the port's PVID. But this is only in cases where untagged frames arrive on tagged ports. Otherwise, the PVID of a port is ignored on a tagged port.

General Rules to Creating a Tagged VLAN

Below is a summary of the rules to observe when creating a tagged VLAN.

- ☐ Each tagged VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches or stacks, each part of the VLAN on the different switches or stacks must be assigned the same VID.
- ☐ A tagged port can be a member of multiple VLANs.
- ☐ An untagged port can be an untagged member of only one VLAN at a time.
- ☐ The ports on an AT-8400 line card can belong to the same VLAN or different VLANs.
- ☐ A port cannot be an untagged and tagged member of the same VLAN.
- ☐ An AT-8400 Series switch can support up to 256 VLANs.

**Tagged VLAN
Example**

Figure 60 illustrates how tagged ports can be used to interconnect IEEE 802.1Q-based products.

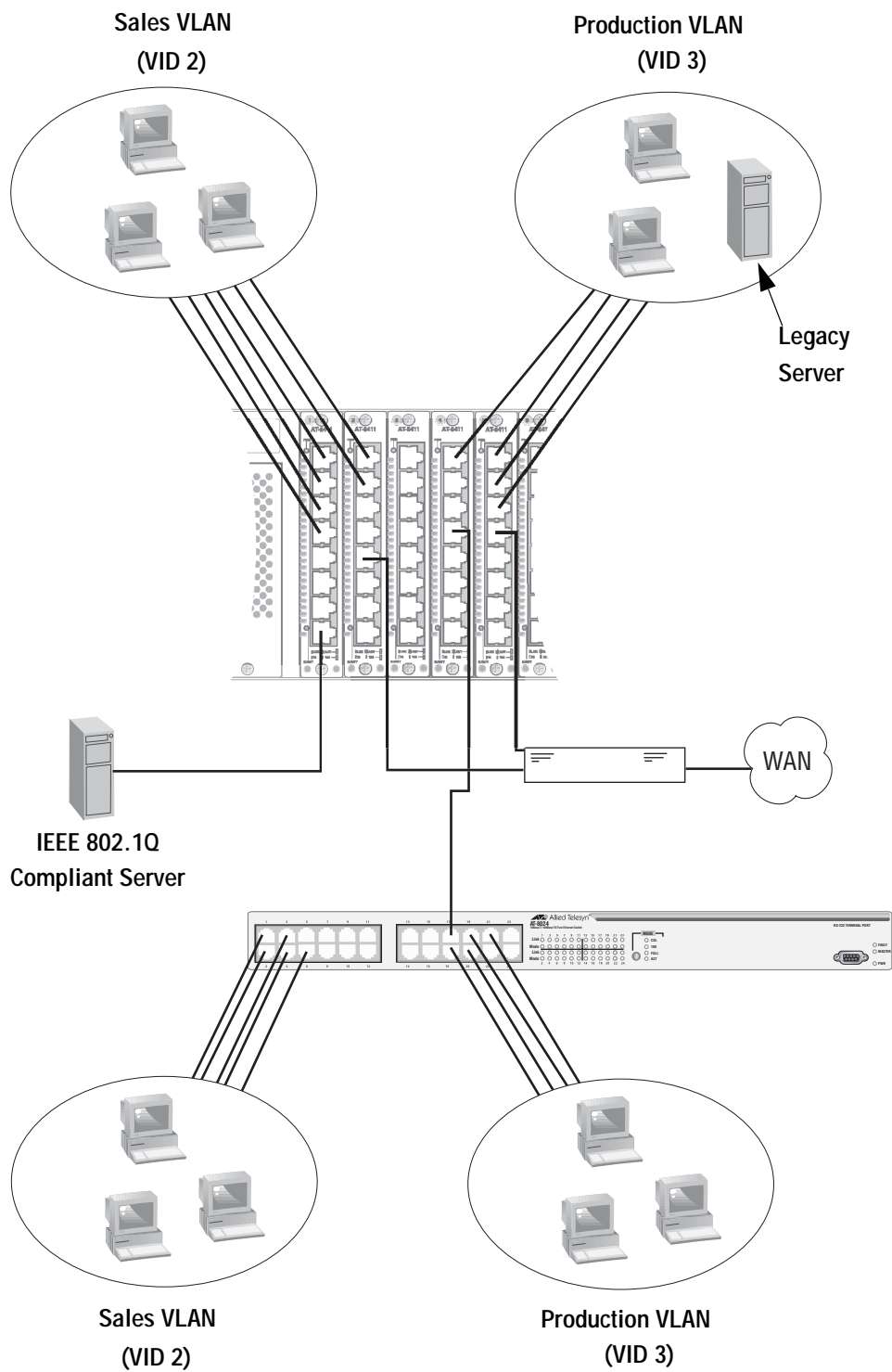


Figure 60 Example of a Tagged VLAN

This example is nearly identical to the port-based VLAN Example 2 earlier in this chapter. Tagged ports have been added to simplify network implementation and management.

The port assignments for the VLANs are as follows:

	Sales VLAN (VID 2)		Production VLAN (VID 3)	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-8400 Switch	Slot 1 Ports: 1 - 4	Slot 1 Port: 8	Slot 4 Port: 1	Slot 1 Port: 8
	Slot 2 Ports: 1 - 2, 5	Slot 4 Port 4	Slot 5 Ports: 1 - 4	Slot 4 Port 4
AT-8024 Switch	1 - 4, 6	17	18 - 21	17

One of the changes is the addition of an IEEE 802.1Q-compliant server. This server can handle frames from multiple VLANs. It is connected to Port 8 on the AT-8411 line card in Slot 1 of the AT-8400 Series switch. Port 8 has been made a tagged port of both the Sales and Production VLANs. This allows the workstations of the VLANs to access the server without having to use the router.

It is important to note that even though the server accepts frames from and transmits frames to more than one VLAN, data separation and security remain. The frames from the server to the switch contain VID information that tell the switch which VLAN the packet belongs to. This prevents packets from crossing VLAN boundaries.

Another use of tagged ports in the example eliminates the need for separate, dedicated links to connect together VLANs that span multiple switches. Back in the port-based **Example 2** on page 177, the Sales and Production VLANs each had separate links to connect together their different parts.

But in this example, tagged ports allow one data link to carry packets from different VLANs, but network security is maintained. Tagged frames, when received by the switch, are delivered only to those ports that belong to the VLAN from which the frames originated.

This shared data link is provided by Port 4 on the AT-8411 line card in Slot 4 of the AT-8400 Series switch and by Port 17 on the AT-8024 switch. Both ports have been made tagged ports of both the Sales VLAN and the Production VLAN.

Each VLAN still has a dedicated connection to the router for access by the Sales VLAN to the legacy server, and also so the two VLANs can access the WAN.

Basic VLAN Mode Overview

The Fast Ethernet Switches support a special VLAN configuration referred to as Basic VLAN Mode. When the Basic VLAN Mode is activated, frames are forwarded based solely on MAC addresses. All VLAN information, including PVIDs assigned to ports and VLAN tags in tagged frames, is ignored. Tagged frames are analyzed only for priority level.

Packets are passed through the switch unchanged. Tagged and untagged frames exit the switch the same as they entered, either tagged or untagged, regardless of the type of ports on which the frames are received and transmitted.

You should be aware of the following before you activate the Basic VLAN mode:

- ❑ If a packet received on a switch port contains a MAC address not already stored in the MAC address table, the packet is flooded out all ports in the AT-8400 Series switch, except for the port on which the packet was received.
- ❑ You can create and modify port-based or tagged VLANs when the Basic VLAN Mode is activated, but the VLANs will not be active. Port-based and tagged VLANs are active only when the switch is operating in the Tagged mode. Additionally, pre-existing port-based or tagged VLANs are retained in the event you later disabled Basic VLAN Mode, but the VLANs are not used.

Note

For instructions on how to activate the Basic VLAN mode, refer to **Setting a Switch's VLAN Mode** on page 197.

Displaying VLANs

This procedure displays all the port-based and tagged VLANs that currently exist on the AT-8400 Series switch. To view the VLANs, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.

The VLAN Menu is displayed in Figure 61.

```
Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager
                               VLAN Menu

1 - Configure VLAN
2 - Display VLAN

R - Return to Previous Menu

Enter your selection?
```

Figure 61 VLAN Menu

2. From the VLAN Menu, type **2** to select Display VLAN.

The Display VLAN menu is displayed in Figure 62.

```
Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager
                               Display VLAN

1 - Display VLAN
2 - Display Management VLAN

R - Return to Previous Menu

Enter your selection?
```

Figure 62 Display VLAN Menu

3. From the Display VLAN menu, type **1** to select Display VLAN.
The Display VLAN window appears. An example of the window is shown in Figure 65.

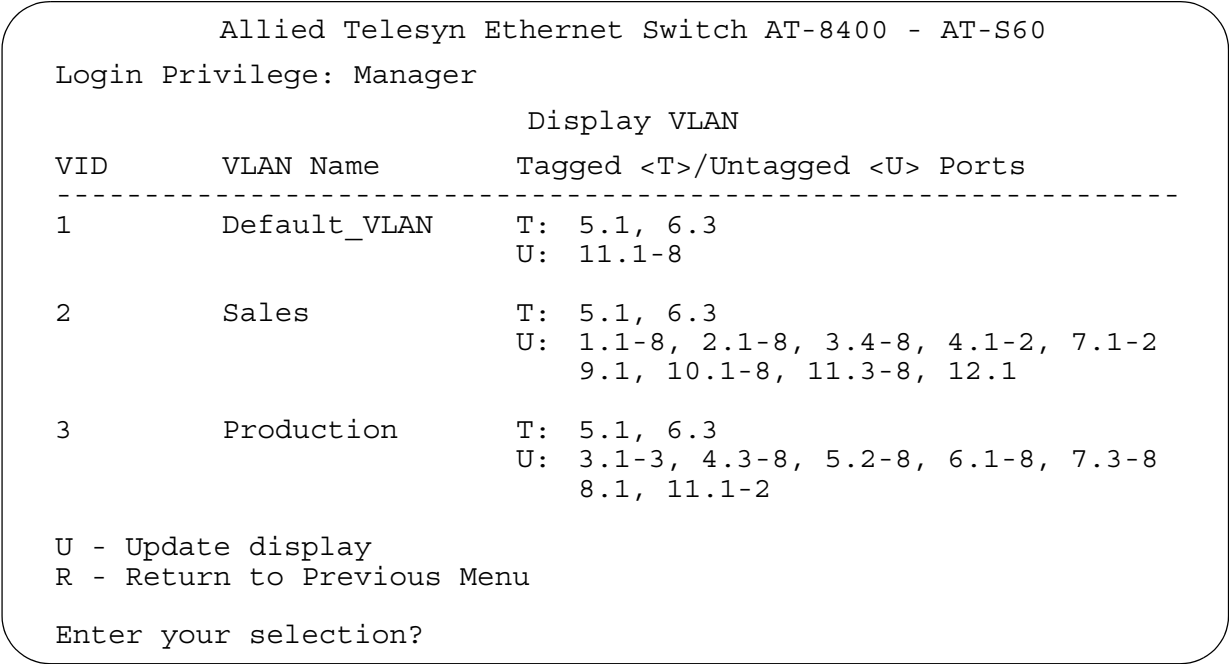


Figure 63 Display VLAN Window

This window displays all the tagged and port-based VLANs that currently exist on the AT-8400 Series switch. The window displays the VID and name of each VLAN, along with the tagged and untagged ports of the VLANs. If you have not created any VLANs, this window will contain only the Default_VLAN.

Creating a Port-based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is displayed in Figure 61 on page 185.
2. From the VLAN Menu, type **1** to select Configure VLAN.
The Configure VLAN menu is displayed in Figure 64.

```
Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager
                        Configure VLAN

1 - Configure VLAN
2 - Set Management VLAN

D - Reset to Default VLAN
R - Return to Previous Menu

Enter your selection?
```

Figure 64 Configure VLAN Menu

- From the Configure VLAN menu, type **1** to select Configure VLAN.
The Configure VLAN window is displayed in Figure 65.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager

                                Configure VLAN

VID      VLAN Name      Tagged <T>/Untagged <U> Ports
-----
1        Default_VLAN   T:  5.1,  6.3
                        U: 11.1-8

2        Sales          T:  5.1,  6.3
                        U: 1.1-8, 2.1-8, 3.4-8, 4.1-2, 7.1-2
                        9.1, 10.1-8, 11.3-8, 12.1

3        Production     T:  5.1,  6.3
                        U: 3.1-3, 4.3-8, 5.2-8, 6.1-8, 7.3-8
                        8.1, 11.1-2

1 - Create VLAN
2 - Delete VLAN
3 - Modify VLAN

U - Update display
R - Return to Previous Menu

Enter your selection?

```

Figure 65 Configure VLAN Menu

This window displays all the tagged and port-based VLANs that currently exist on the AT-8400 Series switch. Included in the window are the VID and name of each VLAN, along with the tagged and untagged ports of the VLANs. If you have not created any VLANs, this window will contain only the Default_VLAN.

- Type **1** to select Create VLAN.
The following prompt is displayed:

```
Enter VLAN Name:
```

- Enter a name for the new VLAN.

The name can be from one to nineteen characters in length. The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

If the VLAN will be unique in your network, then the name should be unique as well. If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

Note

A VLAN must be assigned a name.

After you have entered a name, the following prompt is displayed:

```
Enter VLAN VID: [2 to 4094]
```

6. Enter a VID value for the new VLAN. The permitted range of the VID value is 2 to 4094.

The management software uses the next available VID number on the switch as the default value. If the VLAN will be unique in your network, then its VID must also be unique. If this VLAN will be part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you should assign the Sales VLAN on each switch the same VID value.

Note

A VLAN must have a VID.

The switch is only aware of the VIDs of the VLANs that exist on the line cards in the chassis. The switch is not aware of the VIDs of other VLANs in your network. You may need to take this into account when selecting a VID for a new VLAN.

For instance, let's assume that you just added an AT-8400 Series switch to an existing network that already has VLANs on other switches that use VIDs 2 through 24. When you start to create your first VLAN on the new AT-8400 Series switch, the management software will choose VID 2 to assign to the VLAN, because that is the first VID available on the chassis. It will not automatically know that the VID is already in use by another VLAN on the network.

To avoid inadvertently assigning a new VLAN a VID already being used, you might consider keeping a list of your network VLANs and their associated VIDs.

After you have entered a VID, the following prompt is displayed:

```
Enter Tagged Port-list:
```

7. Specify the tagged ports of the VLAN. If this VLAN will not contain any tagged ports, leave this field empty and simply press Return. For information on entering ports, refer to **Specifying Ports** on page 26.

After you have entered the tagged ports of the VLAN, the following prompt is displayed:

```
Enter Untagged Port-list:
```

8. Specify the ports on the switch to function as untagged ports in the VLAN. If this VLAN will not contain any untagged ports, leave this field empty. For information on entering ports, refer to **Specifying Ports** on page 26.

After you have specified the untagged ports, the management software automatically creates the VLAN. The Configure VLAN window (Figure 65 on page 188) is updated with your new VLAN.

9. Check to see that the VLAN was created correctly and that it contains the appropriate ports.

The new VLAN is now ready for use.

Note

Ports designated as untagged ports of a new VLAN are automatically removed from their current untagged VLAN assignment. For example, if you are creating a new VLAN on a switch that contains only the Default_VLAN, the ports that you specify as untagged ports of the new VLAN are automatically removed from the Default_VLAN.

Tagged ports are not removed from any current VLAN assignments because tagged ports can belong to more than one VLAN at a time.

10. Repeat this procedure starting with Step 4 to create additional VLANs.
11. After you have created all of the VLANs, return to the Main Menu and type **S** to select Save Configuration Changes.

Example of Creating a Port-based VLAN

The following procedure creates the Sales VLAN illustrated in **Port-based Examples** on page 175. This VLAN will be assigned a VID of 2. It will consist of seven untagged ports, Ports 1 to 4 and 8 from the AT-8411 line card in Slot 1 and Ports 1 and 2 from the AT-8411 line card in Slot 2. The VLAN will not contain any tagged ports.

To create the example Sales VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is displayed in Figure 61 on page 185.
2. From the VLAN Menu, type **1** to select Configure VLAN.
The Configure VLAN menu is displayed in Figure 64 on page 187.
3. From the Configure VLAN menu, type **1** to select Configure VLAN.
The Configure VLAN window is displayed in Figure 65 on page 188.
4. Type **1** to select Create VLAN.
The following prompt is displayed:
Enter VLAN Name:
5. Enter "Sales". Press Return.
The following prompt is displayed:
Enter VID [2 to 4094]:
6. Enter "2". This is the VID value for the new VLAN. Press Return.
The following prompt is displayed:
Enter Tagged Port-list:
7. Since the Sales VLAN will not contain any tagged ports, you do not enter any ports for this prompt. You just press Return.
The following prompt is displayed:
Enter Untagged Port-list:
8. Enter "1.1-4,8,2.1-2". These are the untagged ports of the Sales VLAN.
The management software automatically creates the new VLAN and adds it to the list of VLANS in the window.
9. Return to the Main Menu and type **S** to select Save Configuration Changes.

Example of Creating a Tagged VLAN

The following procedure creates the Production VLAN in the AT-8400 Series switch illustrated in **Tagged VLAN Example** on page 182. This VLAN will be assigned the VID 3. It will consist of five untagged ports: Port 1 from the AT-8411 line card in slot 5 and Ports 1 to 4 from the AT-8411 line card in Slot 6. The VLAN will also consist of two tagged ports: Port 8 from Slot 1, which gives the VLAN access to an IEEE 802.1q-compliant server, and Port 4 from Slot 4, which is a shared link to the AT-8024 switch, where another part of the Production VLAN resides.

To create the Production VLAN example, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is displayed in Figure 61 on page 185.
2. From the VLAN Menu, type **1** to select Configure VLAN.
The Configure VLAN menu is displayed in Figure 64 on page 187.
3. From the Configure VLAN menu, type **1** to select Configure VLAN.
The Configure VLAN window is displayed in Figure 65 on page 188
4. Type **1** to select Create VLAN.
The following prompt is displayed:
Enter VLAN Name :
5. Enter "Production". Press Return.
The following prompt is displayed:
Enter VID [2 to 4094] :
6. Enter "3". This is the VID value for the new VLAN. Press Return. The following prompt is displayed:
Enter Tagged Port-list :
7. Enter "1.8,4.4"
These are the tagged ports of the Production VLAN. Port 8 on the line card in Slot 1 is connected to an IEEE 802.1q-compliant server. Port 4 on the line card in Slot 4 is a shared link to the AT-8024 switch, where more nodes of the Production VLAN reside. The following prompt is displayed:
Enter Untagged Port-list :
8. Enter "4.1,5.1-4". These are the untagged ports of Production VLAN.
The management software automatically creates the new VLAN and adds it to the list of VLANS in the window.
9. Return to the Main Menu and type **S** to select Save Configuration Changes.

Modifying a VLAN

The section contains the procedure for adding or deleting ports from a tagged or port-based VLAN.

To modify a VLAN, perform the following procedure:

1. From the Configure VLAN menu, type **3** to select Modify VLAN.

The Modify VLAN menu is displayed in Figure 66.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager

                                Modify VLAN
VID      VLAN Name              Tagged <T>/Untagged <U> Ports
-----
1        Default_VLAN          T:
                                U: 5.1,11.1-8

2        Sales                 T: 5.1
                                U: 1.1-8, 2.1-8, 3.4-8, 4.1-2, 6.3,
                                7.1-2, 9.1, 10.1-8, 11.3-8, 12.1

3        Production            T: 5.1, 6.3
                                U: 3.1-3, 4.3-8, 5.2-8, 6.1-8, 7.3-8
                                8.1, 11.1-2

1 - Add Ports to VLAN
2 - Delete Ports from VLAN
3 - Set Ports to VLAN
4 - Clear Ports from VLAN

U - Update display
R - Return to Previous Menu

Enter your selection?

```

Figure 66 Modifying VLAN Menu

The window displays the tagged and port-based VLANs on the AT-8400 Series switch.

To add ports to a VLAN, go to step 2. To remove ports, go to step 3. To remove ports while assigning new ports, go to step 4. To remove all ports without assigning new ports, go to step 5.

2. To add ports to the VLAN, do the following:
 - a. Type **1** to select Add Ports to VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

- b. Enter the VID of the VLAN you want to change.

The following prompt is displayed:

Enter Tagged Port-list to add:

- c. If you want to add one or more tagged ports to the VLAN, enter them at this prompt. If you are not adding tagged ports, just press Return. For information on entering ports, refer to **Specifying Ports** on page 26.

The following prompt is displayed:

Enter Untagged Port-list to add:

- d. If you want to add one or more untagged ports to the VLAN, enter them at this prompt. If you are not adding untagged ports, just press Return.

Changes are immediately activated on the VLAN.

Note

Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Adding a tagged port to a VLAN does not effect the tagged port's current VLAN assignments.

- e. Repeat this step to modify other VLANs.
3. To remove ports from the VLAN, do the following:

- a. Type **2** to select Delete Ports from VLAN.

The following prompt is displayed:

Enter VLAN ID: [2 to 4094] ->

- b. Enter the VID of the VLAN you want to change.

The following prompt is displayed:

Enter Tagged Port-list to delete:

- c. If you want to remove one or more tagged ports from the VLAN, enter the ports at this prompt. If you are not removing tagged ports, just press Return. For information on entering ports, refer to **Specifying Ports** on page 26.

The following prompt is displayed:

Enter Untagged Port-list to delete:

- d. If you want to remove one or more untagged ports from the VLAN, enter them at this prompt. If you are not removing untagged ports, just press Return.

Changes are immediately activated on the VLAN.

Note

Untagged ports that are removed from a VLAN are automatically returned to the Default_VLAN.

You cannot remove an untagged port directly from the Default_VLAN. Instead, you must assign it as an untagged port to another VLAN.

- e. Repeat this step to modify other VLANs.
4. To remove all ports from a VLAN while assigning new ports, do the following:
 - a. Type **3** to select Set Ports to VLAN.
The following prompt is displayed:
`Enter VLAN ID: [2 to 4094] ->`
 - b. Enter the VID of the VLAN you want to change.
The following prompt is displayed:
`Enter Tagged Port-list:`
 - c. Enter the new tagged ports for the VLAN. To remove all tagged ports without assigning new ports, just press Return.
The following prompt is displayed:
`Enter Untagged Port-list:`
 - d. Enter the new untagged ports from the VLAN. To remove all untagged ports without assigning new ports, just press Return.
Changes are immediately activated on the VLAN.
5. To remove all ports from the VLAN, do the following:
 - a. Type **4** to select Clear Ports from VLAN.
The following prompt is displayed:
`Enter VLAN ID: [2 to 4094] ->`
 - b. Enter the VID of the VLAN you want to change.
All tagged and untagged ports are removed from the VLAN.
6. After modifying the VLANs, return to the Main Menu and type **S** to select Save Configuration Changes.

Deleting a VLAN

To delete a VLAN, perform the following procedure:

1. From the Configure VLAN menu, type **2** to select Delete VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

2. Enter the VID of the VLAN you want to delete and press Return.

Note

You cannot delete the Default_VLAN, which has a VID of 1.

The following confirmation prompt is displayed:

```
Do you want to delete this VLAN? <Y/N>: [Yes/No] ->
```

3. Type **Y** to delete the VLAN or **N** to cancel the procedure. Press Return.

The VLAN has been deleted. All untagged ports in the deleted VLAN are returned to the Default_VLAN as untagged ports.

4. Repeat this procedure to delete additional VLANs.
5. Return to the Main Menu and type **S** to select Save Configuration Changes.

Setting a Switch's VLAN Mode

This section contains the procedure for setting a switch's VLAN mode. You can configure a switch to support port-based and tagged VLANs or to operate in the Basic VLAN mode. Port-based and tagged VLANs and the Basic VLAN mode are described in earlier sections in this chapter.

Note

Changing a switch's VLAN mode will reset the switch. The switch will not forward traffic during the brief period required to reload the AT-S60 management software.

To configure a switch's VLAN mode, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
2. From the System Menu, type **1** to select Configure System.
The Configure System menu is displayed.
3. Type **1** to toggle the Switch Mode setting as desired.
Option 1 - Switch Mode in the Configure Switch menu toggles the switch between port-based and tagged VLANs and the Basic VLAN mode. When the option is showing Tagged, the switch supports port-based and tagged VLANs. When the option is showing Basic, the switch is operating in the Basic VLAN mode.

The system displays the following prompt:

```
Changing the switch mode requires the switch to
reboot:
Do you want to proceed? [Yes/No]
```

4. Type **Y** to change the switch VLAN mode or **N** to cancel this procedure.

If you responded with Y for yes, the switch automatically resets and your management sessions is ended. To continue managing the switch, you must reestablish your management session once the switch has completed reloading the AT-S60 management software.

Specifying a Management VLAN

The management VLAN is the VLAN through which an AT-8400 Series switch expects to receive management packets. This VLAN is important if you are using the enhanced stacking feature of the switch or if you will be managing a switch remotely.

Management packets are packets generated by a management workstation while managing a switch. The management card in the switch will act upon the packets only if they are received on the management VLAN.

The default management VLAN on an AT-8400 Series switch is the Default_VLAN. If you do not create any additional VLANs and link the switches together using untagged ports, then there will be no need to specify a new management VLAN. You should be able to manage all of the AT-8400 Series switches in your network using the enhanced stacking feature.

However, if you create additional VLANs on your switches, it may be necessary for you to create a management communications path and then specify that path as the new management VLAN.

Below are several rules to observe when using this feature:

- ☐ The management VLAN must exist on each AT-8400 Series switch that you want to manage.
- ☐ Using the following procedure, you must specify the management VLAN in the AT-S60 software on each slave and master switch of an enhanced stack.
- ☐ The uplink and downlink ports on the switch that are the data links between the switches must be untagged members of the management VLAN.
- ☐ The port on the switch to which the management station is connected must be an untagged member of the management VLAN. (This does not apply if the management station is connected to the RS-232 port on the management card.)

Here is an example. Let's assume that you have an enhanced stack of three AT-8400 Series switches with one master switch. If the uplink and downlink ports between the various switches are untagged members of the Default_VLAN and if the management station is connected to a untagged port of the Default_VLAN, you can manage all the switches since the Default_VLAN is by default the management VLAN.

Now let's assume that you decided to create a VLAN called NMS with a VID of 24 for the sole purpose of remote network management. For this, you would need to create the NMS VLAN on each AT-8400 Series switch that you want to manage remotely, being sure to assign each NMS VLAN the VID of 24. You would need to be sure that the uplink and downlink ports connecting the switches together are untagged members of the NMS VLAN. And you would also need to specify the NMS VLAN as the management VLAN on each switch using the management software. Finally, you must be sure to connect your management station to a port on a switch that is an untagged member of the management VLAN. (This last step does not apply if you are managing the enhanced stack through the RS-232 port on the management card in one of the switches.)

To specify the management VLAN in the AT-S60 software, do the following:

1. From the Main Menu, type **2** to select VLAN Menu.
2. From the VLAN Menu, type **1** to select Configure VLAN.
3. From the Configure VLAN menu, type **2** to select Set Management VLAN.

The following prompt is displayed:

```
Enter Management VLAN ID [1 to 4094] ->
```

4. Specify the VID of the VLAN that will function as the management VLAN.

Note

The VLAN must already exist on the switch.

The following prompt is displayed:

```
SUCCESS - Press any key to continue...
```

5. Press any key.
6. Return to the Main Menu and type **S** to select Save Configuration Changes.

Chapter 11

MAC Address Table

This chapter provides an overview of MAC addresses. In addition, it describes the procedures for viewing the static and dynamic MAC address table using a local or Telnet management session. This chapter contains the following sections:

- ❑ **MAC Address Overview** on page 201
- ❑ **Displaying MAC Addresses** on page 203
- ❑ **Adding Static MAC Addresses** on page 207
- ❑ **Deleting MAC Addresses** on page 209
- ❑ **Changing the Aging Time** on page 211

MAC Address Overview

Every hardware device that you connect to your network has a unique MAC address associated with it. A MAC address is assigned to a device by the device's manufacturer. For example, every network interface card that you use to connect your computers to your network has a MAC address assigned to it by the adapter's manufacturer.

The AT-8400 Series switch has a MAC address table. The switch uses the table to store the MAC addresses of the network nodes connected to its ports, along with the port number on which each address was learned. The table can store up to 8000 addresses.

The switch learns the MAC addresses of the end nodes by examining the source address of every packet received on a port. It adds the address and port on which the packet was received to the MAC table if the address has not already been entered in the table. The result is a table that contains all the MAC addresses of the devices that are connected to the switch's ports, and the port number where each address was learned.

When the switch receives a packet, it also examines the destination address and, by referring to its MAC address table, determines the port where the destination node is connected. It then forwards the packet to the appropriate port and on to the end node. This increases network bandwidth by limiting each frame to the appropriate port when the intended end node is located, freeing the other switch ports for receiving and transmitting data.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all the ports on the switch. If the ports have been grouped into virtual LANs, the switch floods the packet only to those ports which belong to the same VLAN as the port on which the packet was received. This prevents packets from being forwarded onto inappropriate LAN segments and increases network security. When the destination node responds, the switch adds its MAC address and port number to the table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Since both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

The type of MAC address described above is referred to as a *dynamic MAC address*. Dynamic MAC addresses are addresses that the switch learns by examining the source MAC addresses of the frames received on the ports.

Dynamic MAC addresses are not stored indefinitely in the MAC address table. The switch deletes a dynamic MAC address from the table if it does not receive any frames from the node over a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be purged from the table. This prevents the MAC address table from becoming filled with addresses of nodes that are no longer active.

The period of time that the switch waits before purging an inactive dynamic MAC address is called the *aging timer*. This value is adjustable on the AT-8400 Series switch. The default value is 300 seconds (5 minutes). For instructions on changing the aging timer, refer to **Changing the Aging Time** on page 211.

The MAC address table can also store *static MAC addresses*. A static MAC address, once entered in the table, remains in the table indefinitely and is never deleted, even when the end node is inactive.

You might need to enter static MAC addresses of end nodes the switch might not learn in its normal dynamic learning process. You could also enter a static MAC address so that the address remains permanently in the table, even when the end node is inactive.

Displaying MAC Addresses

The management software has menu selections for displaying all or parts of the MAC addresses table of the AT-8400 Series switch.

To display the MAC address table, perform the following procedure:

1. From the Main Menu, type **7** to select MAC Address Tables.

The MAC Address Tables menu is displayed in Figure 67.

```
Allied Telesyn AT-8400 Series - AT-S60
Login Privilege: Manager

                MAC Address Tables

1 - Configure MAC Addresses
2 - Display MAC Addresses

R - Return to Previous Menu

Enter your selection?
```

Figure 67 MAC Address Tables Menu

2. Type **2** to select Display MAC Addresses.

The Display MAC Addresses menu is shown in Figure 68.

```
Allied Telesyn AT-8400 Series - AT-S60
Login Privilege: Manager

                Display MAC Addresses

1 - Display all MAC Addresses
2 - Display all static MAC Address
3 - Display MAC addresses by Port
4 - Display the port of MAC address
5 - Display MAC addresses by VLAN ID
6 - Display Multicast MAC Addresses

R - Return to Previous Menu

Enter your selection?
```

Figure 68 Display MAC Addresses Menu

3. Select the desired option. Each option is described below:

1 - Display All MAC Addresses

This option displays the Display All MAC Addresses window. This window lists all the switch's dynamic and static address, including multicast addresses. An example of the window is shown in Figure 69.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Session: Manager

                Display All MAC Addresses
Total Number of MAC Addresses: 212
VlanID      MAC                               Port      Type
-----
1           00:a0:d2:18:1a:c8                1.1       Dynamic
1           00:a0:c4:16:3b:80                1.2       Dynamic
1           00:a0:12:c2:10:c6                1.3       Dynamic
1           00:a0:c2:09:10:d8                1.4       Dynamic
1           00:a0:33:43:a1:87                1.5       Dynamic
1           00:a0:12:a7:14:68                1.6       Dynamic
1           00:a0:d2:22:15:10                1.7       Dynamic
1           00:a0:d4:18:a6:89                1.8       Dynamic

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 69 Show All MAC Addresses Window

The columns in the window are defined in Table 5.

Table 5 Columns in the Display All MAC Addresses Window

Column	Definition
VlanID	The VID of the port where the MAC address was learned.
MAC Address	The dynamic, static, or multicast MAC address.
Port	The port where the address was learned (dynamic) or assigned (static).
TYPE	The type of MAC address: dynamic, static, or multicast.

2 - Display All static MAC Addresses

This option displays only the static MAC addresses. The columns in the window are the same as those in the Display All MAC Addresses window. For definitions of the columns, refer to Table 5 on page 204.

3 - Display MAC addresses by Port

You can use this option to view the MAC addresses that have been learned on a particular port. When you select this option, the following prompt is displayed:

```
Enter port-list:
```

Enter the ports. For information on entering ports, refer to **Specifying Ports** on page 26. The management software responds by listing only those addresses learned on the specified ports.

4 - Display the Port of MAC Address

In some situations, you might want to know which port learned a particular MAC address. You could display the entire MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding it could prove difficult.

Instead, you can use this option. When you select this option, the following prompt is displayed:

```
Please enter MAC address:
```

After you enter the MAC address and press Return, the following prompt is displayed:

```
Please enter a VLAN ID: [1 to 4094] ->
```

Enter a VLAN ID and press Return. Then the management software displays the number of the port where it learned the address.

5 - Display MAC Addresses by VLAN ID

This option is useful if you created VLANs on the switch and want to view the MAC addresses of the nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default VLAN, in which case displaying the entire MAC address table, produces the same result.)

To use this option, you need to know the VID number of the VLAN whose MAC addresses you want to view. (To view VLAN VIDs, refer to **Displaying VLANs** on page 185.) When you select the option, the following prompt is displayed:

```
Please enter a VLAN ID: [1 to 4094] ->
```

After you have entered the VID and press Return, the management software displays all of the static and dynamic MAC address of the corresponding VLAN.

6 - Display Multicast MAC Addresses

This selection displays the multicast MAC addresses. For definitions of the columns, refer to Table 5 on page 204.

Adding Static MAC Addresses

This section contains the procedure for adding static addresses to the switch. A MAC address added to the table with this procedure remains permanently in the table, even when the source end node is inactive. You can assign up to 255 static MAC addresses per port on the AT-8400 Series switch.

Note

The switch does not support static multicast addresses.

To add a static or multicast address to the MAC address table, perform the following procedure:

1. From the Main Menu, type **7** to select MAC Address Tables.
The MAC Address Tables window is displayed in Figure 67 on page 203.
2. From the MAC Address Tables menu, type **1** to select Configure MAC Addresses.

The Configure MAC Addresses menu is displayed in Figure 70.

```
Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager
                Configure MAC Addresses
1 - Add static MAC Addresses
2 - Delete MAC Address
3 - Delete all dynamic MAC addresses

R - Return to Previous Menu

Enter your selection?
```

Figure 70 Configure MAC Addresses Menu

3. From the Configure MAC Addressed menu, type **1** to select Add Static MAC Addresses.

The following prompt is displayed:

```
Please enter MAC address ->
```

4. Enter the static MAC address in the following format:

```
xxxxxx xxxxxx
```

Once you have specified the MAC address, the following prompt is displayed:

```
Enter port-list:
```

5. Enter the number of the port on the switch where you want the address assigned.

The management software adds the address to the MAC address table.

6. Repeat this procedure starting with step 3 to enter additional static or multicast MAC addresses.
7. Return to the Main Menu and type **S** to select Save Configuration Changes.

Deleting MAC Addresses

This section contains the procedure for deleting static, dynamic, and multicast MAC addresses from the MAC address table and for purging the table of all dynamic addresses.

To delete MAC addresses from the table, perform the following procedure:

1. From the Main Menu, type **7** to select MAC Address Tables.
The MAC Address Tables menu is displayed in Figure 67 on page 203.
2. From the MAC Address Tables menu, type **1** to select Configure MAC Addresses.
The Configure MAC Addresses menu is displayed in Figure 70 on page 207.
3. To delete a MAC address from the table, do the following:
 - a. From the Configure MAC Addressed menu, type **2** to select Delete MAC Address.
The following prompt is displayed:

```
Please enter a MAC address ->
```
 - b. Enter the MAC address you want deleted from the table in the following format:

```
XXXXXX XXXXXX
```

Note

You cannot delete the switch's MAC address.

The address is immediately deleted from the table.

- c. Repeat the procedure to delete additional MAC addresses.
- d. Return to the Main Menu and type **S** to select Save Configuration Changes.

4. To delete all dynamic MAC addresses from the table, do the following:
 - a. From the Configure MAC Addressed menu, type **3** to select Delete All dynamic MAC Addresses.

The following prompt is displayed:

```
All learned MAC (non-static) addresses will be
deleted.
```

```
Do you want to continue? [Yes/No] ->
```

- b. Type **Y** for yes to delete the dynamic MAC addresses or **N** for no to cancel the procedure.

If you type **Y** for yes, all dynamic MAC addresses are deleted from the MAC address table. The switch immediately begins to relearn the addresses and to add them to the table.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 128 seconds (2 minutes, 8 seconds).

To adjust the aging time, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
2. From the System Menu, type **1** to select Configure System.
3. From the Configure System menu, type **4** to select MAC Address Aging Time.

The following prompt is displayed:

```
Enter MAC address aging timer -> [8 to 512]
```

4. Enter a new value in seconds.

The new value is immediately activated on the switch.

5. Return to the Main Menu and type **S** to select Save Configuration Changes.

Chapter 12

Class of Service

This chapter describes the class of service feature. In addition, it describes the procedures for configuring the Class of Service (CoS) feature of the AT-S60 software using a local or Telnet management session. This chapter contains the following sections:

- ❑ **Class of Service Overview** on page 213
- ❑ **Configuring CoS** on page 214

Class of Service Overview

The AT-8400 Series switch supports CoS as specified in the IEEE 802.1p and 802.1Q standards. CoS can be important in network environments where there are time-critical applications, such as voice transmission or video conferencing, that can be adversely affected by packet transfer delays.

Prior to CoS, network traffic was handled in a best-effort manner. File transfer delays did occur, but were mostly transparent to network users. But with the introduction of time-critical applications, packet transfer delays can prove problematic. For example, transfer delays of voice transmission can result in poor audio quality.

CoS was designed to address this problem. The 802.1p standard outlines eight levels of priority, 0 to 7, with 0 the lowest priority and 7 the highest.

The AT-8400 Series switch has two priority queues, low and high. When a tagged packet enters a switch port, the switch responds by placing the packet into one of the two queues according to following assignments:

IEEE 802.1p Priority Levels	AT-8400 Series switch Queue
7	high
6	high
5	high
4	high
3	low
2	low
1	low
0	low

For example, a tagged packet with a priority tag of 6 is placed in the high priority queue, while a packet with a priority tag of 1 is placed in the low priority queue.

These priority-to-queue assignments can be overridden using the AT-S60 management software on a per port basis.

You can also use CoS to control which priority queue handles untagged frames that ingress a port. By default, untagged frames (i.e., frames without VLAN or priority level information) are automatically assigned to the low priority buffer. But you can configure CoS on a port so that all untagged frames received on the port are directed to the high priority queue.

Configuring CoS

To configure CoS for a port, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **1** to select Port Configuration. The following prompt is displayed:
`Enter port-list:`
3. Enter the port you want to configure. You can enter more than one port at a time. For information on entering ports, refer to **Specifying Ports** on page 26.

The Port Configuration menu for the selected port(s) is displayed. Option 3 controls CoS.
4. Type **3** to toggle Option 3 - Override Priority through the possible settings. The settings are:
 - ☐ No Override - At this setting, which is the default, all untagged packets are directed to the low priority queue, tagged packets with a priority of 0 to 3 are directed to the low priority queue, and tagged packets with a priority of 4 to 7 are directed to the high priority queue.
 - ☐ Low Priority - All tagged and untagged packets are directed to the low priority queue.
 - ☐ High Priority - All tagged and untagged packets are directed to the high priority queue.
5. After setting a port's priority, return to the Main Menu and type **S** to select Save Configuration Changes.

Note

The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered, regardless of the priority queue that handled the frame.

Note

To view the priority queue assignment for a port, use the Port Status selection in the Port Menu.

Chapter 13

IGMP Snooping

This chapter provides a description of the Internet Group Management Protocol (IGMP) snooping feature. Also, it explains how to activate and configure the IGMP snooping feature on the switch using a local or Telnet management session. This chapter contains the following sections:

- ❑ **IGMP Snooping Overview** on page 216
- ❑ **Activating IGMP Snooping** on page 218
- ❑ **Displaying a List of Host Nodes** on page 220
- ❑ **Displaying a List of Multicast Routers** on page 221

IGMP Snooping Overview

IGMP enables routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node wanting to become a member of a particular multicast group responds to a query by sending a *report* which indicates an end node's intention to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. Once a host node has been made a member of a multicast group, it must continue to periodically issue reports to remain a member.

Once the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets out the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

There are two versions of IGMP, referred to as Version 1 and Version 2. One of the differences between the two versions is how a host node indicates that it no longer wants to be a member of a multicast group. In Version 1, it simply stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, the router assumes that the host node no longer wants to receive multicast frames and removes it from the membership list of the multicast group.

In Version 2, a host node exits from a multicast group by sending a *leave request*. Once a router receives a leave request from a host node, it removes the node from the appropriate membership list. If it determines there are no further host nodes on the port, the router also stops sending out multicast packets from the port connected to the node.

IGMP snooping enables the Fast Ethernet switch to monitor the flow of queries from a router and reports from host nodes to build its own multicast membership lists. The switch uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping, a switch would flood multicast packets from all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact switch and network performance.

The AT-8400 Series switch supports both IGMP Version 1 and Version 2. The switch maintains its multicast groups through an adjustable time-out value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note

The default setting for IGMP snooping is disabled.

Activating IGMP Snooping

To activate or deactivate IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
2. From the System Menu, type **1** to select Configure System.
3. From the Configure System window, type **6** to select Configure IGMP Snooping.

The IGMP Snooping Configuration menu is shown in Figure 71.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager
                                Configure IGMP Snooping

1 - IGMP Snooping Status ..... Disabled
2 - Multicast Host Topology ..... Single-Host/Port (Edge)
3 - Host/Router Timeout Interval . 260 seconds
4 - Maximum Multicast Groups ..... 256
5 - View Multicast Hosts List
6 - View Multicast Router List

R - Return to Previous Men

Enter your selection:

```

Figure 71 IGMP Snooping Configuration Menu

The options in the window are defined below:

1 - IGMP Snooping Status

Enables and disables IGMP snooping on the switch. After selecting this option, type **E** to enable or **D** to disable this feature. The default is disabled.

2 - Multicast Host Topology

Defines whether there is one host node per switch port or multiple host nodes per port. Possible settings are Single-Host/Port (Edge) and Multi-Host/Port (Intermediate).

The Single-Host/Port setting is appropriate when there is only one host node connected to a port on the switch. With this setting, the switch immediately stops sending multicast packets out from a switch port when a host node issues a leave request or when a host node stops sending reports.

The Multi-Host setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub where multiple host nodes are connected. With this setting, the switch continues sending multicast packets out from a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port will continue to receive the multicast packets. Only after all the host nodes connected to a switch port have transmitted leave requests (or have timed out) will the switch stop sending multicast packets out from the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through another switch or hub, you should select the Multi-Host Port (Intermediate) selection.

3 - Host/Router Timeout Interval

Specifies the time period, in seconds, after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch watches for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes the router is no longer active on the port.

4 - Maximum Multicast Groups

Specifies the maximum number of multicast groups the switch will learn. The range is 1 to 2048 groups. The default is 256 multicast groups.

This parameter is useful with networks containing a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from becoming filled with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

Note

Selections 5 and 6 in the menu are discussed later in this chapter.

4. After making the desired changes, return to the Main Menu and type **S** to select Save Configuration Changes.

Your changes are activated immediately on the switch.

Displaying a List of Host Nodes

This procedure displays a list of the multicast groups on a switch, as well as the host nodes. To display the list, perform the following procedure:

1. From the IGMP Snooping Configuration window, type **5** to select View Multicast Host List.

(For instructions on how to display the IGMP Snooping Configuration window, perform Steps 1 to 4 of **Activating IGMP Snooping** on page 218.)

The View Multicast Host List is shown in Figure 72.

```

Allied Telesyn Ethernet Switch AT-8400 AT-S60
Login Privilege: Manager

View Multicast Hosts List

=====
MulticastGroup VLAN          Port  HostIP  Status
=====

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 72 View Multicast Hosts List Window

The information in this window is for viewing purposes only. The columns are defined below:

Multicast Group

The multicast address of the group.

VLAN

The VID of the VLAN where the port is an untagged member.

Membership Port

A port on the switch where one or more host nodes of the multicast group are connected.

HostIP

The IP address(es) of the host node(s) connected to the port.

Status

The status of the host node. The status can be either Active, meaning the node is an active member of a multicast group, or Left Group, meaning the node has recently left the group.

Displaying a List of Multicast Routers

A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. You can use the AT-S60 software to display a list of the multicast routers that are connected to the switch.

To display a list of the multicast routers, perform the following procedure:

1. From the IGMP Snooping Configuration window, type **6** to select View Multicast Router List.

(For instructions on how to display the IGMP Snooping Configuration window, perform Steps 1 to 4 of **Activating IGMP Snooping** on page 218.)

The View Multicast Router List in Figure 72 is displayed.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager
      View Multicast Routers List

=====
Port          VLAN          RouterIP
=====

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 73 View Multicast Routers List Window

The information in this window is for viewing purposes only. The columns are defined below:

Port

A port on the switch connected to a multicast router.

VLAN

The VID of the VLAN where the port is an untagged member.

RouterIP

The IP address of the multicast router.

Chapter 14

Ethernet Statistics

This chapter contains the procedures for displaying data traffic statistics using a local or Telnet management session. It contains the following section:

- ❑ **Displaying Port Statistics** on page 223

Displaying Port Statistics

To display Ethernet port statistics, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu

From the Port Menu, type **3** to select Port Statistics. The Ethernet Statistics menu in Figure 74 is displayed.

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manager

                        Port Statistics

1 - Display Port Statistics
2 - Clear Port Statistics

R - Return to Previous Menu

Enter your selection?
  
```

Figure 74 Port Statistics Menu

2. Type **1** to select Display Port Statistics.

The following prompt is displayed:

```
Enter port-list:
```

3. Enter the port whose statistics you want to view. You can specify more than one port at a time. For information on entering ports, refer to **Specifying Ports** on page 26.

A window is displayed containing the port statistics. The information in this window is for viewing purposes only. The statistics are defined below:

Bytes Received

Number of bytes received on the port.

Bytes Sent

Number of bytes transmitted from the port.

Frames Received

Number of frames received on the port.

Frames Sent

Number of frames transmitted from the port.

Broadcast Frames Received

Number of broadcast frames received on the port.

Broadcast Frames Sent

Number of broadcast frames transmitted from the port.

Multicast Frames Received

Number of multicast frames received on the port.

Multicast Frames Sent

Number of multicast frames transmitted from the port.

Frames 64 Bytes**Frames 65 - 127 Bytes****Frames 128 - 255 Bytes****Frames 256 - 511 Bytes****Frames 512 - 1023 Bytes****Frames > 1024 Bytes**

Number of frames transmitted from the port, grouped by size.

CRC Error

Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Jabber

Number of occurrences of corrupted data or useless signals appearing on the port.

Fragments

Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received on the port.

Dropped Frames

Number of frames successfully received and buffered by the port, but discarded and not forwarded.

Collisions

Number of collisions that have occurred on the port.

Late Collisions

Number of collisions that have occurred late in the transmission of a frame.

Undersize Frames

Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Oversize Frames

Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

4. If you want to clear the counters on the port and return them to "0", select option "2 - Clear Statistics" from the Port Statistics menu.

Chapter 15

File Downloads and Uploads

This chapter contains information on obtaining AT-S60 software updates. The chapter also contains procedures on how to download and upload files to a switch from a local or Telnet management session. It includes the following sections:

- ❑ **Overview** on page 226
- ❑ **Obtaining Software Updates** on page 228
- ❑ **Transferring Files from a Local Management Session** on page 229
- ❑ **Transferring Files from a Telnet Session** on page 234
- ❑ **Downloading Files Switch to Switch** on page 237
- ❑ **Uploading Files** on page 239

Overview

There are three files that coexist on an AT-8400 chassis. They are:

- ❑ AT-S60 management software image

This is the operating software for the switch.

- ❑ AT-S60 bootloader

This image contains the code that initially controls the switch when powered on or reset.

- ❑ Switch configuration file

This file contains the settings for the different switch parameters, such as VLANs, port trunks, and so forth.

You can use the AT-S60 management software to download new versions of the management software and bootloader onto a switch so that a switch always has the latest software.

You can also upload a configuration file from a switch onto a management workstation and then download it onto another switch. This can be useful in network environments that contain a large number of AT-8400 chassis that will all be configured the same, or nearly the same. You can configure one AT-8400 chassis in your network, and then download its configuration file to the other switches. This can save you from having to configure each switch individually.

There are several different ways to download and upload files onto a switch. They are:

- ❑ Local management session

This method is performed from a local management session using either Xmodem or TFTP. The procedure for this is described in **Transferring Files from a Local Management Session** on page 229.

- ❑ Telnet management station

This method is performed from a remote Telnet management session using TFTP. The procedure for this is described in **Transferring Files from a Telnet Session** on page 234.

❑ Switch to switch

You can perform this procedure from either a local or remote management session. It is particularly useful if your network contains a large number of AT-8400 chassis. You can upgrade the software on one master switch and then instruct the master switch to upgrade the software in the other switches in the same subnet. This procedure is explained in **Downloading Files Switch to Switch** on page 237.

Obtaining Software Updates

New releases of the AT-S60 management software are available from the Allied Telesyn web site at www.alliedtelesyn.com and our FTP server at [ftp.alliedtelesyn.com](ftp://ftp.alliedtelesyn.com). To log on to the FTP server, enter "anonymous" for the user name and your email address for the password. Management software for the AT-8400 chassis has "S60" as part of the filename.

Transferring Files from a Local Management Session

This section contains the procedure for downloading the following files onto a switch from a local management session.

- ☐ New AT-S60 software image and bootloader software
- ☐ Configuration file

You can transfer a file using Xmodem or TFTP. In order to use TFTP, there must be a node on your network with the TFTP server software and the file to download must be stored on that node.



Caution

The switch will stop forwarding Ethernet traffic during the download and initialization of the AT-S60 software image.

Note

Installing a new AT-S60 software image does not change the current configuration settings of a switch (e.g., IP address, subnet mask, and virtual LANs).

This procedure assumes that you have already obtained the new AT-S60 software from Allied Telesyn and stored it on the management workstation from which you will be performing the procedure, or on the TFTP server.

Note

To download new software onto the switch using TFTP, your network must have a server or workstation with the TFTP server software. You must store the new AT-S60 image on that server or workstation.

To download a new software image or configuration file onto a switch, perform the following procedure:

1. Establish a local management session on the switch where you intend to download the new management software or configuration file.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The following menu is displayed:

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manger
                        Downloads & Uploads

1 - Download Application Image/Bootloader
2 - Download Configuration Data

3 - Upload Application Image/Bootloader
4 - Upload Configuration Data

R - Return to Previous Menu

Enter your selection?

```

Figure 75 Downloads & Uploads Menu

Note

Menu options 3 and 4 in the menu are described in **Uploading Files** on page 239.

4. To download a new software image and bootloader onto the switch, type **1**. To download a configuration file, type **2**.

The following prompt is displayed:

```
Download Method/Protocol [X-Xmodem, T-TFTP] :
```

5. To download a file using Xmodem, go to Step 6. To download a file using TFTP, do the following:
 - a. Type **T**.

The following prompt is displayed:

```
TFTP Server IP address:
```

- b. Enter the IP address of the TFTP server.

The following prompt is displayed:

```
Remote File Name:
```

- c. Enter the directory path and file name of the image file or configuration file that you want to download.

Note

The image file or configuration file must be stored on the TFTP server.

Once the filename has been specified, the download begins. Downloading a configuration file takes only a few moments; however, downloading an AT-S60 image file can take several minutes.

If you are installing a new management image, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch automatically resets.

Note

Do not interrupt the initialization process. Do not reboot the switch.

6. To download a file using Xmodem, type **X** at the prompt displayed in Step 4.

The following prompt is displayed:

```
You are going to invoke the Xmodem download utility.
Do you wish to continue? [Yes/No]
```

7. Type **Y** for Yes.

The prompt "Downloading" is displayed.

8. Begin the file transfer of the new management software image.

Note

The transfer protocol must be Xmodem or 1K Xmodem.

Steps 9 through 12 illustrate how you would download a file using the Hilgraeve HyperTerminal program.

9. From the HyperTerminal main window, select the **Transfer** menu. Then select **Send File** from the pull-down menu, as shown in Figure 76.

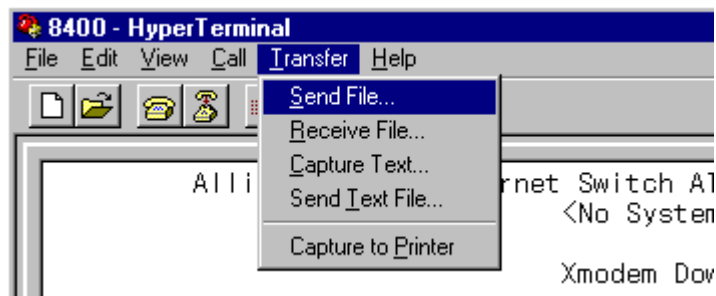


Figure 76 Transfer Menu

The Send File menu in Figure 77 is displayed.

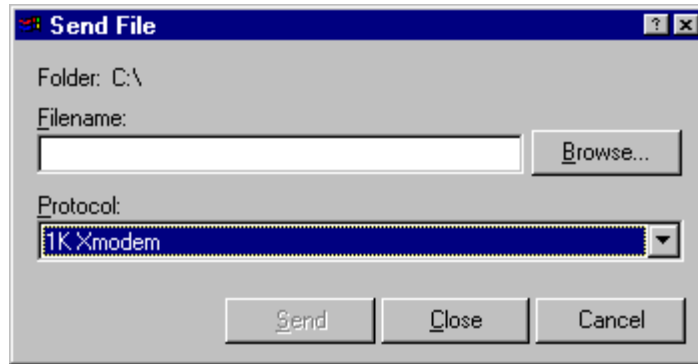


Figure 77 Send File Menu

10. Click the Browse button and specify the location and file to be downloaded onto the switch.
11. Click on the Protocol field and select as the transfer protocol either Xmodem or, for a faster download, 1K XModem.
12. Click Send.

The software immediately begins to download onto the switch. The Xmodem File Send window in Figure 78 displays current status of the software download. The download process takes a couple minutes to complete.

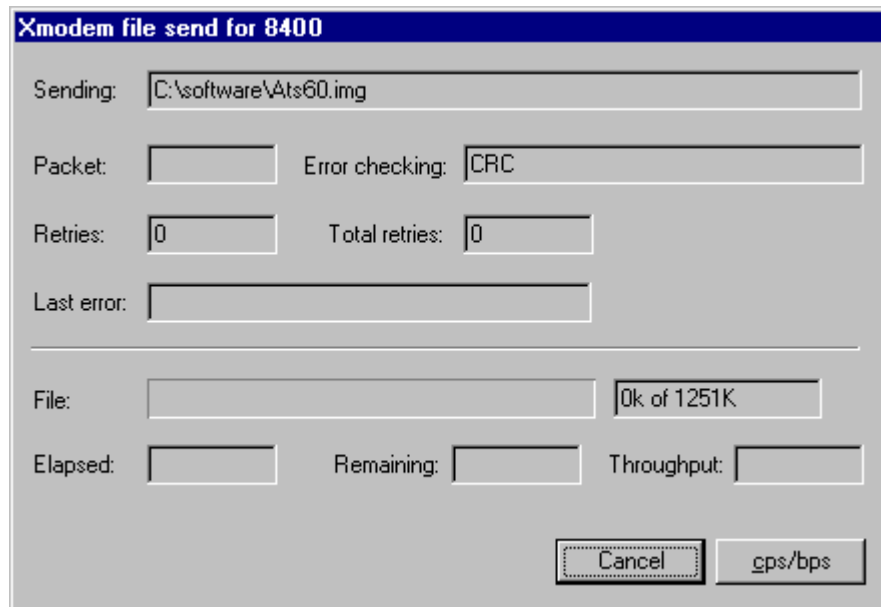


Figure 78 XModem File Send Window

If you are installing a new management image, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch automatically resets.

Note

Do not interrupt the initialization process. Do not reboot the switch.

Transferring Files from a Telnet Session

This section contains the procedure for downloading or uploading the following files onto a switch from a Telnet session.

- ☐ New AT-S60 software image and bootloader software
- ☐ Configuration file

Note

Your network must have a server or workstation with the TFTP server software. You must store the new AT-S60 image or configuration file on that server or workstation.



Caution

The switch will stop forwarding Ethernet traffic during the download of the AT-S60 software image.

Note

Installing a new AT-S60 software image does not change the current configuration of a switch (e.g., IP address, subnet mask, and virtual LANs).

This procedure assumes that you have already obtained the new software from Allied Telesyn and stored it on the TFTP server.

To download a new software image or configuration file onto a switch, perform the following procedure:

1. Establish a Telnet management session on the switch where you intend to download the new management software or configuration file.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The following menu is displayed:

```

Allied Telesyn Ethernet Switch AT-8400 - AT-S60
Login Privilege: Manger
                        Downloads & Uploads

1 - Download Application Image/Bootloader
2 - Download Configuration Data

3 - Upload Application Image
4 - Upload Configuration Data

R - Return to Previous Menu

Enter your selection?

```

Figure 79 Downloads & Uploads Menu

Note

Options 3 and 4 in the menu are described in **Uploading Files** on page 239.

4. To download a new software image and bootloader onto the switch, type **1**. To download a configuration file, type **2**.

The following prompt is displayed:

```
Download Method/Protocol [T-TFTP]:
```

5. Type **T**.

The following prompt is displayed:

```
TFTP Server IP address:
```

6. Enter the IP address of the TFTP server.

The following prompt is displayed:

```
Remote File Name:
```

7. Enter the directory path and file name of the image file or configuration file that you want to download.

Note

The image file and configuration file must be stored on the TFTP server. Additionally, the paths to these files must be specified in the TFTP server.

Once the filename has been specified, the download begins. File download takes only a few moments.

Note

If you are installing a new management image, the switch begins to initialize the software after it is installed, a process that takes approximately one minute to complete. Once the management software is initialized, the switch automatically resets, ending the current Telnet management session. After allowing the switch to reset, you can reestablish the Telnet management session.

Downloading Files Switch to Switch

This procedure explains how to download an AT-S60 software image or configuration file from one AT-8400 chassis to another switch.

This procedure is useful in networks that contain a large number of AT-8400 chassis. Once you have updated the software on the master switch of an enhanced stack, you can instruct the master switch to automatically upgrade the other AT-8400 chassis in the same subnet.

Note

The following procedure can be performed from either a local or Telnet management session.

To download a management software image or configuration file from a master AT-8400 Series switches to other AT-8400 Series switches in the same subnet, perform the following procedure:

1. From the Main Menu, type **8** to select Enhanced Stacking.

The Enhanced Stacking window in Figure 19 on page 72 is displayed.

2. From the Enhanced Stacking window, type **2** to select Stacking Services.

Note

The "2 - Stacking Services" selection is available only from a management session on a master switch.

The window in Figure 20 on page 73 is displayed.

3. From the Stacking Services window, type **1** to select Get/Refresh List of Switches.

The master switch polls the network for all slave and master switches in the subnet and displays a list of the switches in the Stacking Services window. (The list will not include the master switch where you started the management session, or any switches with a stacking status of unavailable.)

4. Do one of the following:
 - ☐ To download both the AT-S60 software image and bootloader on the master switch to another AT-8400 chassis, type **4** to select Image Download Image/Bootloader.

- ❑ To download just the configuration file on the master switch to another AT-8400 chassis, type **5** to select Download Configuration.

A prompt similar to the following is displayed:

```
Enter the remote switch number -> [1 to 12]
```

5. Enter the number (Num column in window) of the AT-8400 Series switches whose software or configuration file you want to update. You can specify more than one switch at a time. You can specify the switches individually (e.g., 2,4,5), as a range (e.g., 3-6), or both (e.g., 1-4,7,10). You can download to up to 64 switches at a time.

Note

You can update only AT-8400 Series switches. You cannot download AT-S60 management software or an AT-8400 configuration file onto an AT-8000 Series switch.

The following prompt is displayed:

```
Do you want to show remote switch burning flash ->
[Yes/No]
```

You can use this prompt to view system messages as the software image is stored to flash memory.

6. You can respond with Yes or No to this prompt. It does not affect the download.

The following prompt is displayed:

```
Do you want confirmation before downloading each
switch -> [Yes/No]
```

7. If you are updating multiple switches, answering Yes to this prompt causes the management software to display a confirmation message before it upgrades a switch. If you answer No, the master switch downloads without a confirmation message.

The management software begins the download. The management software notifies you when the download is complete.



Caution

Once a switch image file has been downloaded, the switch must decompress it and write it to flash memory. This requires one to two minutes to complete. Do not reset or power off the switch while it is decompressing the file. Once the file has been decompressed and initialized, the switch automatically resets.

Uploading Files

To upload a management software image or configuration from a switch onto your management station, perform the following procedure:

Note

Allied Telesyn does not recommend that you upload an AT-S60 software image onto a management workstation for the purpose of downloading it onto another switch. Obtain new AT-S60 software images for downloading onto a switch from the Allied Telesyn web site.

1. Start a local management session on the switch where you intend to upload the management software image or configuration file.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The Downloads and Uploads menu in Figure 75 on page 230 is displayed.

4. To upload the AT-S60 software image and bootloader from the switch, type **3**. To upload a configuration file, type **4**.

The following prompt is displayed:

Upload Method/Protocol [X-Xmodem, T-TFTP] :

5. To upload a file using Xmodem, go to Step 6. To upload a file using TFTP, do the following:

- a. Type **T**.

The following prompt is displayed:

TFTP Server IP address:

- b. Enter the IP address of the TFTP server.

The following prompt is displayed:

Remote File Name:

- c. Enter a file name for the image file or configuration file.

Once a file name has been specified, the upload begins. Uploading a configuration file takes only a few moments; however, uploading an AT-S60 image file can take several minutes.

6. To upload a file using Xmodem, type **X** at the prompt displayed in Step 4.

The following prompt is displayed:

```
You are going to invoke the Xmodem download utility.  
Do you wish to continue? [Yes/No]
```

7. Type **Y** for Yes.

The prompt "Uploading" is displayed.

8. Begin the file transfer of the new management software image.

Note

The transfer protocol must be Xmodem or 1K Xmodem.

Section III

Web Browser Management

The chapters in Section III explain how to manage an AT-8400 switch using a web browser. The chapters include:

- ☐ **Chapter 16, Starting a Web Browser Management Session** on page 242
- ☐ **Chapter 17, Basic Switch Parameters** on page 246
- ☐ **Chapter 18, Enhanced Stacking** on page 265
- ☐ **Chapter 19, Port Parameters** on page 270
- ☐ **Chapter 20, Port Security** on page 282
- ☐ **Chapter 21, Port Trunks** on page 286
- ☐ **Chapter 22, Port Mirroring** on page 292
- ☐ **Chapter 23, STP, RSTP, and MSTP** on page 297
- ☐ **Chapter 24, Virtual LANs** on page 320
- ☐ **Chapter 25, MAC Address Table** on page 329
- ☐ **Chapter 26, IGMP Snooping** on page 337

Chapter 16

Starting a Web Browser Management Session

This chapter contains the procedure for starting a management session on an AT-8400 Series switch using a web browser, such as Microsoft Internet Explorer or Netscape Navigator.

Starting a Web Browser Management Session

This section explains how to start a web browser management session.

To start a web browser management session with the AT-S60 software, there must be at least one AT-8400 Series switch on your network that has been assigned an IP address. The switch with the IP address is referred to as the master switch. Once you have started a web browser management session on the master switch, you will have management access to all other AT-8400 and AT-8000 Series Switches that reside in the same subnet.

Note

For optimal viewing of an AT-S60 Web Browser management session on your PC, Allied Telesyn recommends setting the screen resolution to 1024 x 768 pixels.

There are a total of 14 login sessions available using the console, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The console and Telnet sessions allow a total of 10 active sessions. While a web browser management session, allows four active login sessions.

Note

For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 68.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

Note

If your PC (where the web browser resides) is connected directly to the switch or is on the same side of a firewall as the switch, you must configure your browser's network options to not use proxies. Consult your web browser's documentation on how to configure the switch's web browser to not use proxies.

2. Enter the IP address of the switch in the URL field of the browser, as shown in Figure 80.

Switch's IP Address

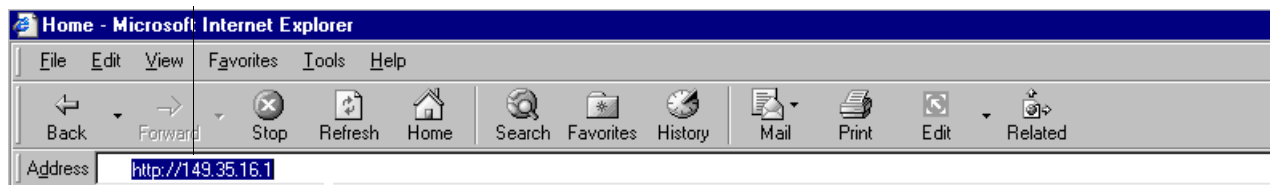


Figure 80 Entering a Switch's IP Address in the URL Field

3. When prompted, enter a user name and password. For information about login ids, see **Management Access Levels** on page 25.

You cannot change the user names. However, you can change the passwords, as explained in **Configuring an IP Address and Switch Name** on page 38.

The Home Page is displayed in Figure 81.

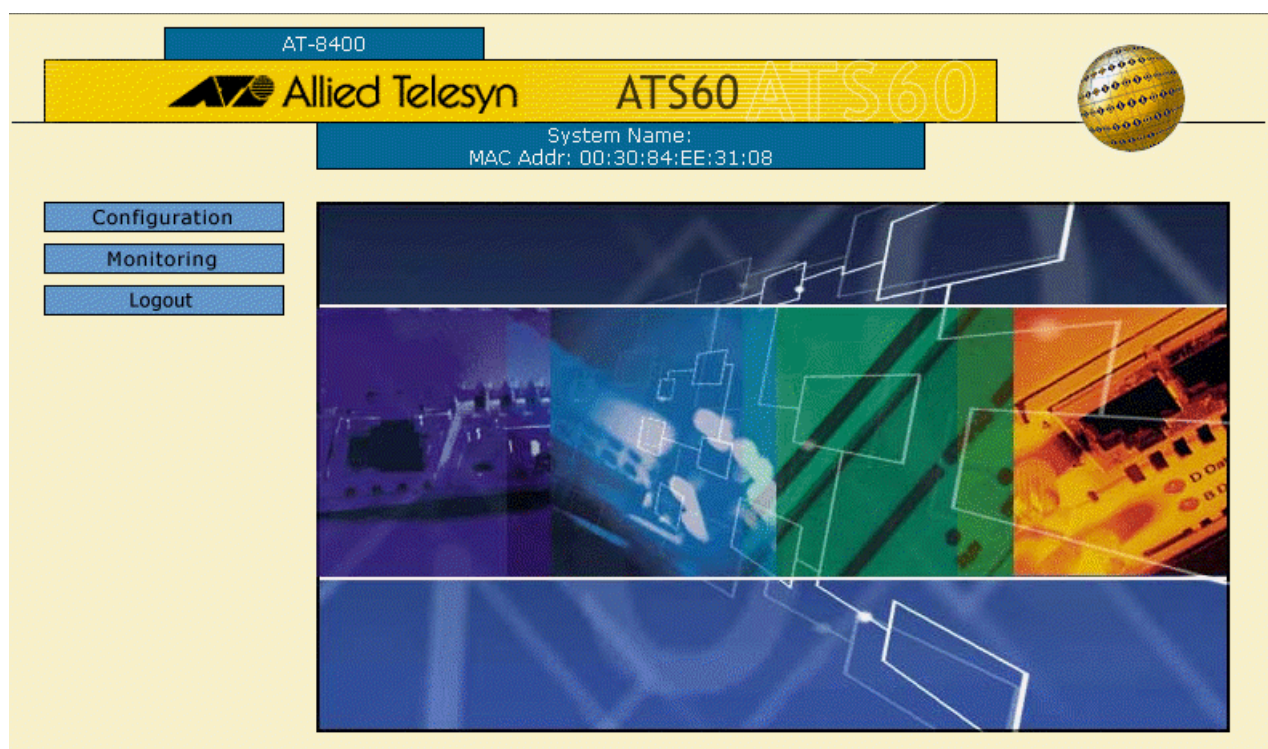


Figure 81 Home Page

Figure 81 shows the Home page of the management software. The main menu is on the left side of the Home page. It consists of the following menus:

- ☐ Configuration
- ☐ Monitoring
- ☐ Logout

Browser Tools

You can use the browser's **bookmark** feature on to record the IP address of the switch.

Note

After 15 minutes of inactivity, a web browser management session times out.

Quitting from a Web Browser Management Session

To exit a web browser management session, select **Logout**.

Chapter 17

Basic Switch Parameters

This chapter provides the following procedures for configuring basic switch parameters using a web browser management session:

- ❑ **Configuring an IP Address and Switch Name** on page 247
- ❑ **Activating the BOOTP and DHCP Services** on page 252
- ❑ **Viewing System Information** on page 253
- ❑ **Configuring the SNMP Parameters and Trap IP Addresses** on page 256
- ❑ **Resetting a Switch** on page 262
- ❑ **Pinging a Remote System** on page 263
- ❑ **Returning the AT-S60 Software to the Factory Default Values** on page 264

Note

For background information regarding basic switch parameters, see on page 35.

Configuring an IP Address and Switch Name

This procedure describes the parameters in the Administration section of the Configuration window. Information about the Configuration and MAC Address Aging Time parameters are discussed later in this guide.

Note

For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-8400 Series switch, refer to **Assigning an IP Address to a Switch** on page 36.

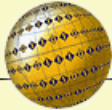
To set the basic switch parameters for an AT-8400 switch, perform the following procedure:

1. From the Home Page, select **Configuration**.
The Configuration System Web Page is displayed with the System menu option selected by default. See Figure 82 on page 248.
2. If the System menu option is not selected, select it and then select the **General** tab.

The Configuration System Web Page is displayed in Figure 82.

AT-8400

Configuration



System Name: High School Switch
MAC Addr: 00:30:84:EE:31:08

Home

System

Layer 1

Layer 2

Help

Logout

General

SNMP

IGMP

Factory Default

Administration

System Name

High School Switch

Administrator

Comments

IP Address

149 . 35 . 16 . 85

Subnet Mask

255 . 255 . 252 . 0

Default Gateway

149 . 35 . 16 . 1

Manager Password

Confirm Manager Password

Operator Password

Confirm Operator Password

Configuration

BOOTP/DHCP

☐ Enable ☒ Disable

Switch Mode

☒ Basic ☐ Tagged

MAC Address Aging Time

300 second(s)

Apply

Defaults

Reset

Figure 82 Configuration System Web Page

Note
The Reset button at the bottom of the window is used to reset the switch.

3. Change the parameters as desired.

The parameters are described below:

System Name

This parameter specifies a name for the switch (for example, Sales Ethernet switch). Entering a value for this parameter is optional.

Note

Allied Telesyn recommends that you assign a name to each switch because switch names help you identify the various switches in your network. Knowing a switch's name ensures you perform a configuration procedure on the correct switch.

Administrator

This parameter specifies the name of the network administrator responsible for managing the switch. Entering a value for this parameter is optional.

Comments

This parameter specifies additional information about the switch, such as its location (for example, Floor 4, Wiring closet 402B). Entering a value for this parameter is optional.



Caution

Changing the IP address of the switch may result in the loss of your management session.

IP Address

This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program. In addition, you must specify an IP address if you want to configure the switch as the master switch of an enhanced stack.

Subnet Mask

This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch.

Default Gateway

This parameter specifies the default router's IP address. You are required to enter a value for this parameter if you will remotely manage the switch from a management station that is separated from the switch by a router.

Manager Password**Manager Confirm Password**

These parameters are used to change the administrator's login password for the switch. The password can be from 0 to 20 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "friend".

**Caution**

Allied Telesyn recommends that you do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in either the Manager or Operator password if you will be managing the switch from a web browser. Many web browsers do not permit special characters in passwords.

Operator Password**Operator Confirm Password**

These parameters are used to change the Operator's password for the switch. The password can be from 0 to 20 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "operator".

BOOTP/DHCP

For information about these parameters, see **Activating the BOOTP and DHCP Services** on page 252.

Switch Mode

Defines the switch's current VLAN mode. If this parameter displays "Tagged," the switch supports port-based and tagged VLANs. If this parameter displays "Basic," the switch is operating in the Basic VLAN Mode. For information about VLANs, refer to the overview sections in **Chapter 10, Virtual LANs on page 168**. For instructions on how to set the switch's VLAN mode from a web browser management session, refer to **Setting the Switch's VLAN Mode on page 328**.

MAC Address Aging Time

For information about this parameter, see **Changing the Aging Time** on page 336.

4. After you have set the parameters, click **Apply**.
5. Click **Save Changes**.

The changes you made are saved on the switch.

Note

Changing any of the above parameters, including the IP address and subnet mask, is immediately activated on the switch.

Changing the IP address of the switch can cause the loss of the remote management session. You can restart the management session using the switch's new IP address.

Activating the BOOTP and DHCP Services

For background information on BOOTP and DHCP, refer to the section **Activating the BOOTP and DHCP Services** on page 45.

To activate or deactivate the BOOTP and DHCP protocols on the switch from a web browser management session, perform the following procedure:

1. From the Home Page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. If the System menu option is not selected, select it and then select the **General** tab.
The General Tab window is displayed, as shown in Figure 82 on page 248.
3. In the BOOTP/DHCP options in the General tab window, click either **Enable** or **Disable**.

Note

If you activate BOOTP/DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

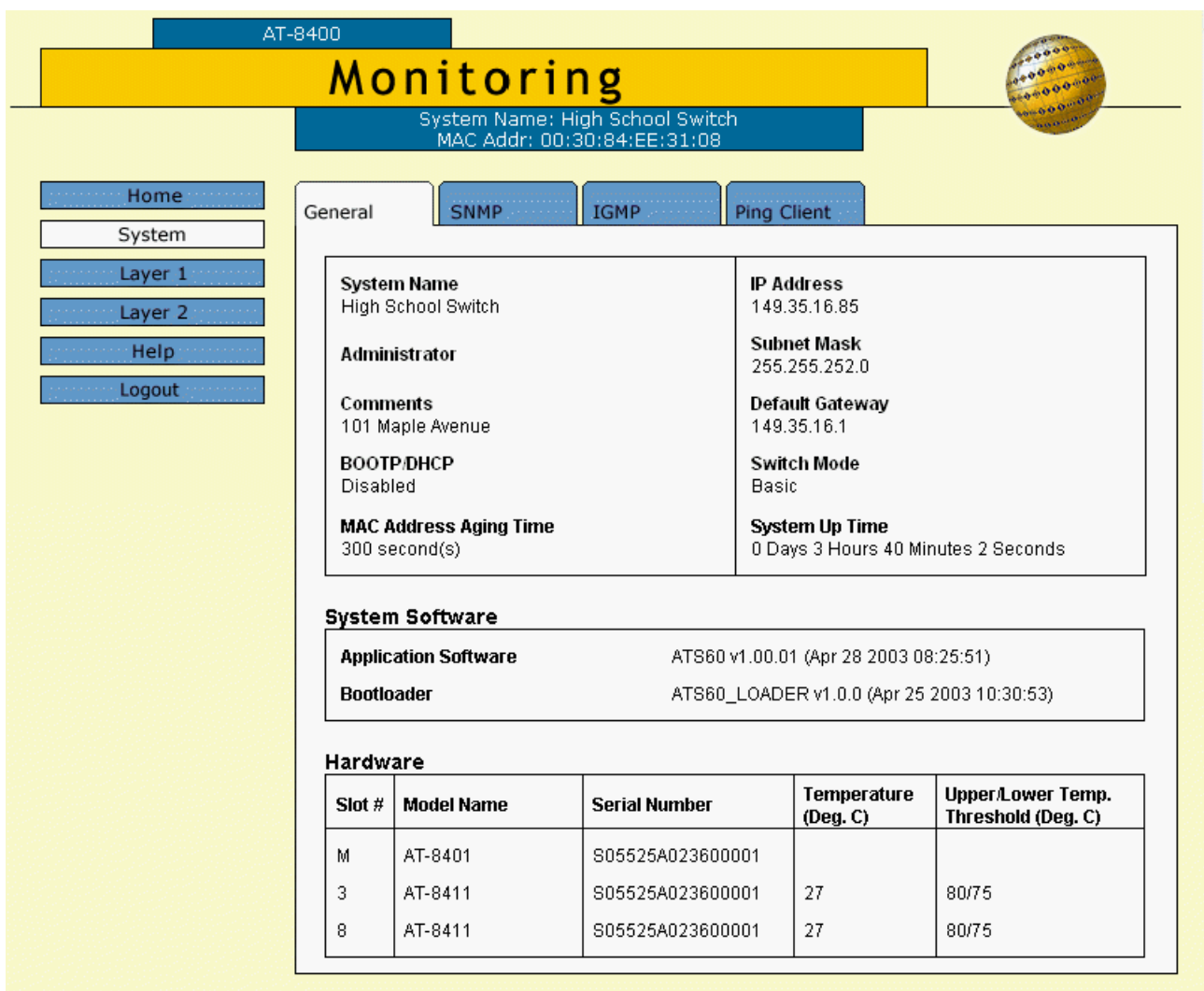
Viewing System Information

To view system information you access the Monitoring window. The parameters on this window are strictly for viewing purposes only. You cannot change any of the values from this window.

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **System**.
3. Select the **General** tab.

The Monitoring Web Page is displayed in Figure 83.



The screenshot shows the 'Monitoring' web page for an AT-8400 switch. The page has a yellow background with a blue navigation bar at the top. The navigation bar includes a 'Home' button, a 'System' button (which is highlighted), and buttons for 'Layer 1', 'Layer 2', 'Help', and 'Logout'. The main content area is titled 'Monitoring' and displays system information for 'High School Switch' with MAC address '00:30:84:EE:31:08'. The 'General' tab is selected, showing fields for System Name, Administrator, Comments, BOOTP/DHCP status, MAC Address Aging Time, IP Address, Subnet Mask, Default Gateway, Switch Mode, and System Up Time. Below this, the 'System Software' section shows the Application Software and Bootloader versions. The 'Hardware' section contains a table with columns for Slot #, Model Name, Serial Number, Temperature (Deg. C), and Upper/Lower Temp. Threshold (Deg. C).

Slot #	Model Name	Serial Number	Temperature (Deg. C)	Upper/Lower Temp. Threshold (Deg. C)
M	AT-8401	S05525A023600001		
3	AT-8411	S05525A023600001	27	80/75
8	AT-8411	S05525A023600001	27	80/75

Figure 83 Monitoring Web Page

The sections in the window are defined below.

General

This section displays the basic switch information. The values cannot be changed at this menu. For the procedure to change the values of the System Name, Administrator, Comments, IP Address, Subnet Mask, and Default Gateway parameters, see **Configuring an IP Address and Switch Name** on page 247.

This section contains the following items:

- ☐ System Name - This parameter specifies a name for the switch (for example, Sales Ethernet switch).
- ☐ Administrator - This parameter specifies the name of the network administrator responsible for managing the switch.
- ☐ Comments - This parameter specifies additional information about the switch, such as its location.
- ☐ BOOTP/DHCP - Defines whether the switch obtains its IP address from a BOOTP or DHCP server on your network. If this parameter is enabled, the switch obtains its IP address from BOOTP or DHCP server.
- ☐ MAC Address Aging Time - Specifies how long an inactive dynamic MAC address can remain in the MAC address table before it is deleted. The default is 300 seconds (5 minutes). For background information about MAC addresses, refer to **MAC Address Overview** on page 201.
- ☐ IP Address - This parameter specifies the IP address of the switch.
- ☐ Subnet Mask - This parameter specifies the subnet mask for the switch.
- ☐ Default Gateway - This parameter specifies the default router's IP address.
- ☐ Switch Mode - Defines the switch's current VLAN mode. If this parameter displays "Tagged," the switch supports port-based and tagged VLANs. If this parameter displays "Basic," the switch is operating in the Basic VLAN Mode. For information about VLANs, refer to the overview sections in **Chapter 10, Virtual LANs** on page 168. For instructions on how to set the switch's VLAN mode from a web browser management session, refer to **Setting a Switch's VLAN Mode** on page 197.
- ☐ System Up Time - The number of days, hours, minutes, and seconds since the switch was rebooted.

System Software

This section contains information about the version of the AT-S60 software and the version of the bootloader.

This section contains the following items:

- ❑ Application Software Information - This parameter lists the current version of the AT-S60 software.
- ❑ Bootloader Information - This parameter lists the current version of the bootloader software.

Hardware

This section contains information about the current line cards and management card installed in the AT-8400 switch.

This section contains a table with the following headings:

- ❑ Slot# - This heading indicates which slot number the line card or management card installed in the chassis. For example, in Figure 83 on page 253 under the heading Slot#, 1 indicates an AT-8411 line card installed in slot 1 of the chassis.
- ❑ Model Name - This heading indicates the name of the line card or management card.
- ❑ Serial Number - This heading indicates the serial number that is printed on the line card or management card.
- ❑ Temperature (Deg. C) - This heading indicates the current temperature, in Celsius, of the line card or management card.
- ❑ Upper/Lower Temp. Threshold (Deg. C) - This heading indicates the current upper and lower temperature thresholds, in Celsius, for the line card.

Configuring the SNMP Parameters and Trap IP Addresses

This procedure allows you to create SNMP communities that have access to the switch. In creating an SNMP community, you can specify up to eight IP addresses of management stations that can access the switch. In addition, you can specify up to eight trap receiver IP addresses of trap receivers that will receive unauthenticated failure trap messages from the switch. The following procedure permits you to modify current SNMP community parameters as well as delete SNMP community access. To save your configuration changes, you must return to the General Tab and click **Save Changes**.

To create, modify, or delete SNMP communities perform the following procedure.

1. From the Home page, select **Configuration**.
2. Select the **SNMP** tab.

The SNMP Web Page is displayed in Figure 84.

AT-8400

Configuration

System Name:
MAC Addr: 00:30:84:EE:31:08

Home
System
Layer 1
Layer 2
Help
Logout

General SNMP IGMP Factory Default

☒ Enable SNMP Access
☒ Enable Authentication Failure Trap

Apply

Total Communities: 2. Page 1 of 1

	Community Name	Access	Manager Stations	Trap Receivers	Status
<input checked="" type="radio"/>	private	Read/Write	192.168.1.101	192.168.1.100, 192.168.1.101	Enabled
<input type="radio"/>	public	Read Only	ALL IP	192.168.1.101	Enabled

Refresh Add Remove Modify

Figure 84 SNMP Web Page

3. Adjust the parameters as desired. The parameters are described below.

Enable SNMP Access

Use this parameter to enable the switch to be remotely managed with an SNMP application program.

Note

If the check box in the Enable SNMP Access box is empty, the switch cannot be managed through SNMP. This is the default.

Enable Authentication Failure Trap

Use this selection to allow trap receiver IP addresses to be specified. When this field is selected and the switch receives an unauthenticated request, an authentication failure trap is sent to the trap receivers configured on the switch.

4. Click **Apply** to display your changes in the Status column of the SNMP Web Page.
5. To add an SNMP Community to the current list, click **Add**.

The Add New SNMP Community Web Page is displayed. See Figure 85.

Add New SNMP Community

Community Name : private2

Status : ☒ Enable ☐ Disable

Access Mode : ☐ Read Only ☒ Read-Write

Managers	Trap Receivers
<input type="checkbox"/> Allow Any Station	
Manager IP Address 1 192.168.1.200	Trap Receiver IP Address 1 192.168.1.200
Manager IP Address 2 	Trap Receiver IP Address 2
Manager IP Address 3 	Trap Receiver IP Address 3
Manager IP Address 4 	Trap Receiver IP Address 4
Manager IP Address 5 	Trap Receiver IP Address 5
Manager IP Address 6 	Trap Receiver IP Address 6
Manager IP Address 7 	Trap Receiver IP Address 7
Manager IP Address 8 	Trap Receiver IP Address 8

Apply Cancel

Figure 85 Add New SNMP Community Web Page

Configure the following parameters:

Community Name

Enter an SNMP community name that consists of up to 15 alphanumeric characters.

Status

Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode

Click Read Only to allow read access to the SNMP community.
Click Read-Write to allow read-write access to the SNMP community.

Allow Any Station

Click this option to allow any SNMP manager to access the switch.
When you click this option, a warning message appears on the screen. Click OK to continue.

Manager IP Address1 through Manager IP Address 8

Enter an IP Address of a switch that is permitted SNMP manager access to the current switch. You can enter up to 8 Manager IP Addresses.

Trap Receiver IP Address 1 through Trap Receiver IP Address 8

Use the above selections to specify the IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

6. Click **Apply** to update the SNMP Web Page.

To save your changes, return to the System Tab and click **Save Changes**.

7. To make changes to a current SNMP community, click on the circle next to the community name on the SNMP Web Page. Then click **Modify**.

The Modify SNMP Web Page is displayed in Figure 86 on page 260.

To save your changes, return to the System Tab and click **Save Changes**.

Modify SNMP Community

Community Name : private

Status : ☒ Enable ☐ Disable

Access Mode : ☐ Read Only ☒ Read-Write

Managers	Trap Receivers
<input type="checkbox"/> Allow Any Station	
Manager IP Address 1 192.168.1.101	Trap Receiver IP Address 1 192.168.1.100
Manager IP Address 2 	Trap Receiver IP Address 2 192.168.1.101
Manager IP Address 3 	Trap Receiver IP Address 3
Manager IP Address 4 	Trap Receiver IP Address 4
Manager IP Address 5 	Trap Receiver IP Address 5
Manager IP Address 6 	Trap Receiver IP Address 6
Manager IP Address 7 	Trap Receiver IP Address 7
Manager IP Address 8 	Trap Receiver IP Address 8

Apply Cancel

Figure 86 Modify SNMP Community Web Page

Configure the following parameters:

Community Name

This field is not configurable from this web page. It is the name of the SNMP community.

Status

Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode

Click **Read Only** to allow read access to the SNMP community.
Click **Read-Write** to allow read-write access to the SNMP community.

Allow Any Station

Click this option to allow any SNMP manager to access the switch.
When you click this option, a warning message appears on the screen. Click **OK** to continue.

Manager IP Address1 through Manager IP Address 8

Enter an IP Address of a switch that is permitted SNMP manager access to the current switch. You can enter up to 8 Manager IP Addresses.

Trap Receiver IP Address 1 through Trap Receiver IP Address 8

Use the above selections to specify the IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

8. Click **Apply** to update the SNMP Web Page.
9. To remove an SNMP community from the list of communities on the SNMP Web Page, click on the circle next to the community name and click **Remove**.

A warning message is displayed. Click **OK** to remove the SNMP community.

10. Click **Apply** to update the SNMP Web Page.
11. Click **System** from the sidebar.

The Configuration Web Page is displayed.

12. Click **Save Changes**.

The changes you made are saved on the switch.

Resetting a Switch

To reset a switch, perform the following procedure:

1. From the Home Page, select **Configuration**.
The Configuration System Web Page is displayed with the System option selected by default.
2. If the System menu option is not selected, select it and then select the **General** tab.
3. Click the **Reset** button at the bottom of the web page.
A confirmation prompt is displayed.
4. Click **OK** to reset the switch or **Cancel** to cancel the procedure.
Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Note

The switch will not forward traffic while it reloads the AT-S60 management software. This will take approximately 30 seconds to complete.

Pinging a Remote System

You can instruct the switch to ping a node on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the Home Page, select **Monitoring**.
2. From the Monitoring window, select the **System** menu option.
3. Select the **Ping Client** tab.

The Ping Client Web Page is displayed in Figure 87.

Figure 87 Ping Client Web Page

4. Enter the IP address of the end node you want the switch to ping.
5. Click **OK**.

The results of the ping are displayed in a new window.

6. To stop the pinging, click **OK**.

Returning the AT-S60 Software to the Factory Default Values

The procedure in this section returns all AT-S60 software parameters, except the IP address, subnet mask, and gateway address, to their default values. This procedure also deletes any VLANs that you have created on the switch.

Note

The AT-S60 software default values can be found in **Appendix A, AT-S60 Default Settings** on page 343.

To return the AT-S60 management software to its default settings, perform the following procedure:

1. From the Home Page, select **Configuration**.
2. Select the **System** menu option.
3. Select the **Factory Default** tab.

The Factory Default Web Page is displayed in Figure 88.

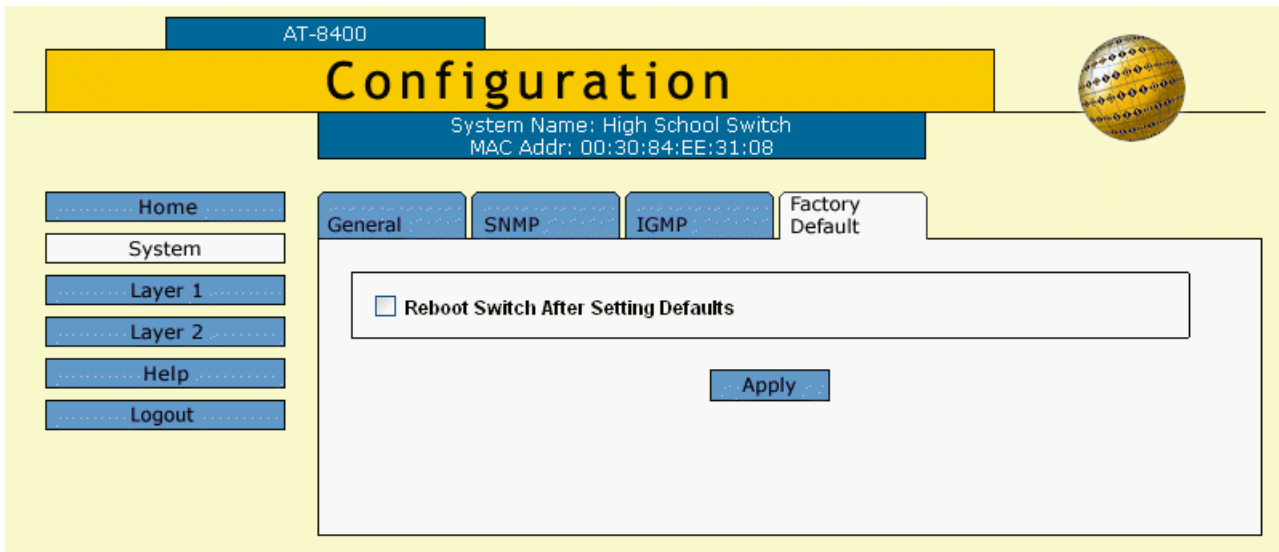


Figure 88 Factory Default Web Page

4. Click the check box next to Reboot Switch After Setting Defaults.
5. Click **Apply**.
6. Follow the prompts.

Chapter 18

Enhanced Stacking

This chapter introduces enhanced stacking, describes how to assign enhanced stacking status to an AT-8400 Series Switch, and describes how to select a remote switch using a web browser management session.

This chapter contains the following sections:

- ❑ **Overview** on page 266
- ❑ **Setting a Switch's Enhanced Stacking Status** on page 266
- ❑ **Selecting a Switch in an Enhanced Stack** on page 267

Note

For background information on enhanced stacking, refer to **Enhanced Stacking Overview** on page 68.

Overview

Using a web browser management session, you can view and set the enhanced stacking status of the switch. In addition, you can view and manage other switches in an enhanced stack. For detailed information about enhanced stacking, see **Enhanced Stacking Overview** on page 68.

The enhanced stacking status of the switch can be master, slave, or unavailable. Each status is described below:

- ☐ **Master** - An AT-8400 switch configured as “master” can be used to manage other AT-8400 and AT-8000 Series Switches in the same subnet.

A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP services on the switch.

- ☐ **Slave** - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask.
- ☐ **Unavailable** - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally.

Note

The default setting for a switch is slave.

Setting a Switch's Enhanced Stacking Status

To adjust a switch's enhanced stacking status, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. Select the **Enhanced Stacking** tab.

The Enhanced Stacking Web Page is displayed in Figure 89.

The screenshot shows the AT-S60 Configuration Web Page. At the top, there is a blue header with 'AT-8400' and a yellow 'Configuration' title bar. Below the title bar, a blue box displays 'System Name: Middle School Switch' and 'MAC Addr: 00:30:84:EE:31:08'. On the left is a sidebar with buttons: Home, System, Layer 1, Layer 2, Help, and Logout. The main content area has tabs for 'MAC Address', 'VLAN', 'Spanning Tree', and 'Enhanced Stacking'. The 'Enhanced Stacking' tab is active, showing a 'Switch State' section with three radio buttons: 'Master' (selected), 'Slave', and 'Unavailable'. An 'Apply' button is at the bottom right of the 'Switch State' section.

Figure 89 Enhanced Stacking Web Page

4. Click the desired enhanced stacking status for the switch.
5. Click **Apply**.
The new enhanced stacking status is immediately activated on the switch.
6. Click **System** from the sidebar.
The Configuration Web Page is displayed.
7. Click **Save Changes**.
The changes you made are saved on the switch.

Selecting a Switch in an Enhanced Stack

You can use the AT-S60 software to access a remote switch from a master switch. The remote switch can be either a slave or a master.

When you start a web browser management session on the master switch, you are addressing only the master switch. Consequently, the management tasks that you perform only affect the master switch. To manage a remote switch in the same subnet, you need to select it from the master switch.

Each switch in a subnet has a unique MAC address. To quickly differentiate between switches in a subnet, Allied Telesyn suggests configuring system names. For example, using system names will help you determine the difference between two AT-8400 switches within the same subnet. For information about how to assign a system name to an AT-8400 switch, see **Configuring an IP Address and Switch Name** on page 247.

Use this procedure to select a remote switch from a master switch. You must configure the AT-8400 switch as a master switch to view the Enhanced Stacking button.

1. From the Home page, select **Enhanced Stacking**.

The Home page appears as shown in Figure 81 on page 244.

Note

If the Home page does not have an Enhanced Stacking button, the switch's enhanced stacking status is either slave or unavailable. For instructions on how to change a switch's stacking status, refer to the previous procedure.

The master switch polls the network for all remote switches in the same subnet and displays a list of the switches in the Stacking Switches web page. See Figure 90.

AT-8400

Enhanced Stacking

System Name: Tech Pubs Switch
MAC Addr: 00:30:84:EE:31:08

Home
Help
Logout

Stacking Switches

Total Switches: 3. Page 1 of 1

	No.	Mac Addr	Name	Switch Mode	Software Version	Switch Model
<input checked="" type="radio"/>	1	00:00:00:AA:BB:CD	8012M	Master	v3.1.1	AT-8012M
<input type="radio"/>	2	00:30:84:52:02:60	SV Users 8	Slave	v3.1.1	AT-8024GB
<input type="radio"/>	3	00:30:86:00:00:00		Slave	v3.1.1	AT-8088/MT

Refresh Connect

Figure 90 Stacking Services Web Page

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC addresses.

You can refresh the list by clicking **Refresh**. This instructs the master switch to poll the subnet for all available switches again.

2. Select the green circle next the switch you want to manage and press **Connect**.

You are prompted to enter the user name and password for the remote switch.

3. Enter the user name and password for the remote switch and click **OK**.

The Home page for the remote switch you selected appears. See Figure 91 on page 269. You can now manage the remote switch.

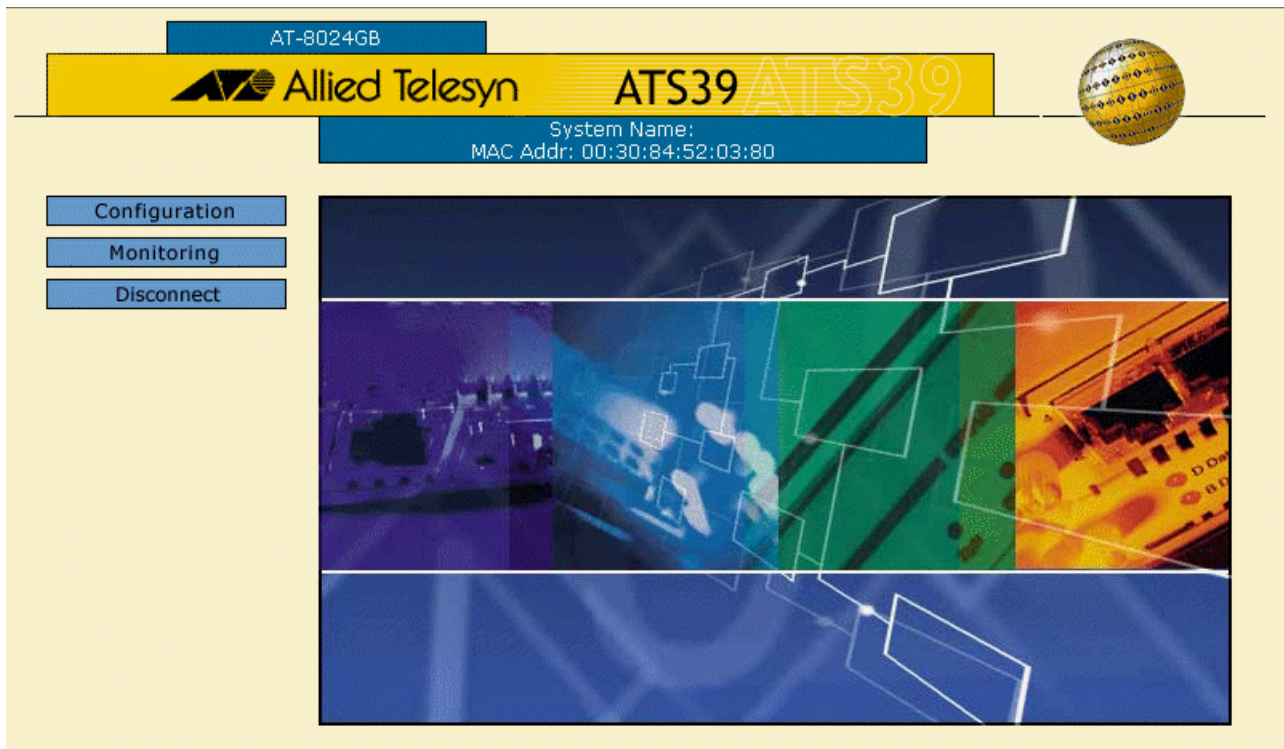


Figure 91 AT-S39 Home Page

4. For information about the remote switch you selected, consult the appropriate Allied Telesyn documentation.

Returning to the Master Switch

When you have finished managing a remote switch, select **Disconnect** from the Home page of the remote switch. This returns you to the Stacking Switches window in Figure 90 on page 268. Once you see that window, you are addressing the master switch again.

You can either select another switch in the list to manage or, to manage the master switch, return to the master switch's Home page by selecting **Home**.

Chapter 19

Port Parameters

The procedures in this chapter allow you to view and change the parameter settings for the individual ports on a switch using a web browser management session. Examples of port parameters that you can adjust include duplex mode and port speed.

This chapter contains the following procedures:

- ❑ **Configuring Port Parameters** on page 271
- ❑ **Displaying Port Status and Statistics** on page 276

Configuring Port Parameters

This procedure describes how to configure one or more ports on an AT-8400 switch. It is important to note that when you select multiple ports for configuration, you are making the same configuration changes on all of the ports.

To configure the parameter settings for a port or ports on a switch, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 1** from the sidebar.
3. Select the **Port Settings** tab.

The Port Settings Web Page is shown in Figure 92.

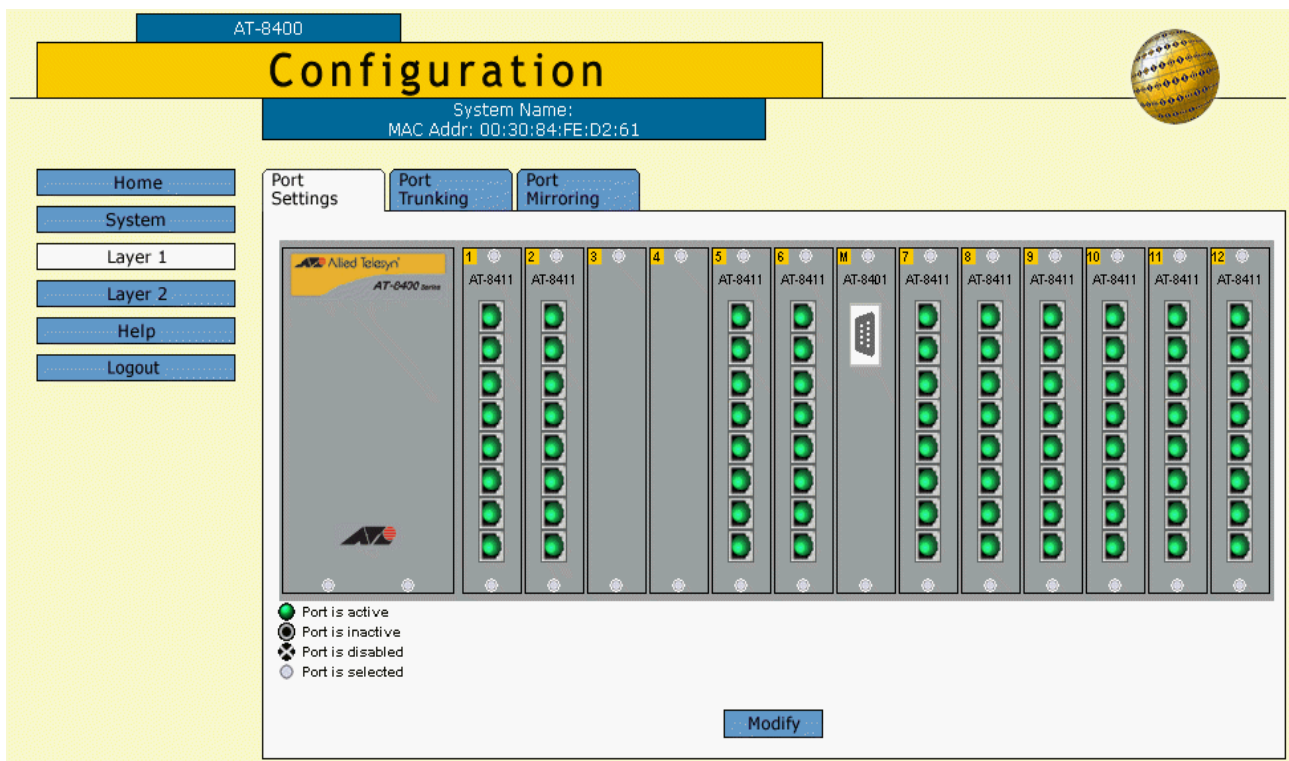


Figure 92 Port Settings Web Page

This page displays a graphical image of the front of the switch. Ports with a valid link to an end node are green.

4. Click on the port or ports that you want to configure. After you click on a port, it turns white. (To deselect a port, click it again.)

**Caution**

Use caution when updating the port that is connected to your management workstation and is communicating with the switch. In making changes to this port, you could inadvertently lose your management session.

5. Click **Modify**.

The Configuring Ports Web Page is displayed as in Figure 93.

Figure 93 Configuring Ports Web Page

Note

Clicking the **Defaults** button returns the port settings to the default values which are listed in **Appendix A, AT-S60 Default Settings** on page 343.

6. Adjust the port parameters as desired.

The parameters are described below.

Port Name:

This is the name of the port or ports you selected for configuration in Step 5. If you selected one port, you can change the port name in this field. However, if you selected more than one port, you cannot change this value. The port(s) you selected appear at the top of the web page. In Figure 93, the port 2.1 was selected.

Speed and Mode

You use this selection to configure a port for Auto-Negotiation or to manually set a port's speed and duplex mode.

To select a value, click the circle next it. Possible values are:

- ☐ Auto-Negotiate: Select Auto-Negotiation to set both speed and duplex mode for the port automatically. This is the default setting.
- ☐ 10 Mbps - Half Duplex: Select this value to set the port or ports to a speed of 10 Mbps and half-duplex mode.
- ☐ 10 Mbps - Full Duplex: Select this value to set the port or ports to a speed of 10 Mbps and full-duplex mode.
- ☐ 100 Mbps - Half Duplex: Select this value to set the port or ports to a speed of 100 Mbps and half-duplex mode.
- ☐ 100 Mbps - Full Duplex: Select this value to set the port or ports to a speed of 100 Mbps and full-duplex mode.
- ☐ 1 GB - Half Duplex: Select this value to set the port or ports to a speed of 1 Gigabit and half-duplex mode.
- ☐ 1 GB - Full Duplex: Select this value to set the port or ports to a speed of 1 Gigabit and full-duplex mode.

HOL Blocking

You use this selection to prevent a packet from being forwarded to a blocking or blocked port. For example, a blocking or blocked port can be one that is receiving too many packets.

To select a value, click the circle next it. Possible values are:

- ☐ Enabled - Indicates HOL blocking is turned on. Packets sent from this port will not be forwarded to a blocked port. This is the default.
- ☐ Disabled - Indicated HOL blocking is turned off. Packets sent from this port will be forwarded to a blocked port.

Override Priority

You use this selection to determine packet priority.

For more information about this feature, refer to **Class of Service Overview** on page 213.

To select a value, click the circle next it. Possible values are:

- ☐ None - Indicated that no override priority is assigned to incoming packets. Instead, the port forwards packets according to the priority embedded in the packet. This is the default.
- ☐ Low - Indicates low priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the low priority queue.
- ☐ High - Indicates high priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the high priority queue.

Status

You use this selection to enable or disable a port. When disabled, a port will not receive or transmit frames.

For example, you may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

To select a value, click the circle next it. Possible values are:

- ☐ Enabled - The port will receive and forward packets. This is the default setting.
- ☐ Disabled - The port will not receive or forward packets.

Broadcast Filter

You use this selection to protect a port from a deluge of packets caused by a broadcast storm. Enabling the broadcast filter parameter on a port causes the port to discard all ingress broadcast frames.

To select a value, click the circle next it. Possible values are:

- ☐ Enabled - The port will discard all ingress broadcast frames.
- ☐ Disabled - The port will accept all ingress broadcast frames. This is the default setting.

Back Pressure

You can use this selection only if the port or ports you specified are operating at half-duplex mode. When you specify that a port is in this mode and it has a packet that is pending transmission, then the software suspends the JAM pattern before sending the packet. After the packet is sent, the JAM pattern resumes.

To select a value, click the circle next it. Possible values are:

- ☐ Enabled - Indicates back pressure is activated on this port. When the port is receiving too many packets, the port will send a signal to the end node to stop sending information.
- ☐ Disabled - Indicates back pressure is not activated on this port. When the port is receiving too many packets, the port will not send a signal to the end node to stop sending information. This is the default.

Flow Control

Flow control applies only to ports operating in full-duplex mode. The switch uses a special pause packet to stop the end node from sending frames. The pause packet notifies the end node to stop transmitting for a specified period of time.

To select a value, click the circle next it. Possible values are:

- ☐ Auto - Indicates the port conforms to the flow control setting of the end node. For example, if flow control is active on the end node then flow control is active on this port. Also, if flow control is not active on the end node, then flow control is not active on this port. This is the default.
- ☐ Disabled - Indicates that no flow control occurs on the port.
- ☐ Enabled - Indicates that flow control occurs on the port.

7. Once you have made the desired changes, click **Apply**.

You are returned to the Port Settings Web Page as shown in Figure 92 on page 271.

8. Click **System** from the sidebar.

The Configuration Web Page is displayed.

9. Click **Save Changes**.

The changes you made are saved on the switch. The switch immediately activates the parameter changes on the port.

Displaying Port Status and Statistics

The procedures in this section display the operating status of the ports on a switch and port statistics. You can view a port's operating speed, duplex mode, MDI/MDI-X configuration, and more. You can also view the operating status of any GBIC modules installed.

Displaying Port Status

To display the status of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring page, select **Layer 1** from the sidebar.
3. Select the **Port Settings** tab. The Port Monitoring Web Page is shown in Figure 94.

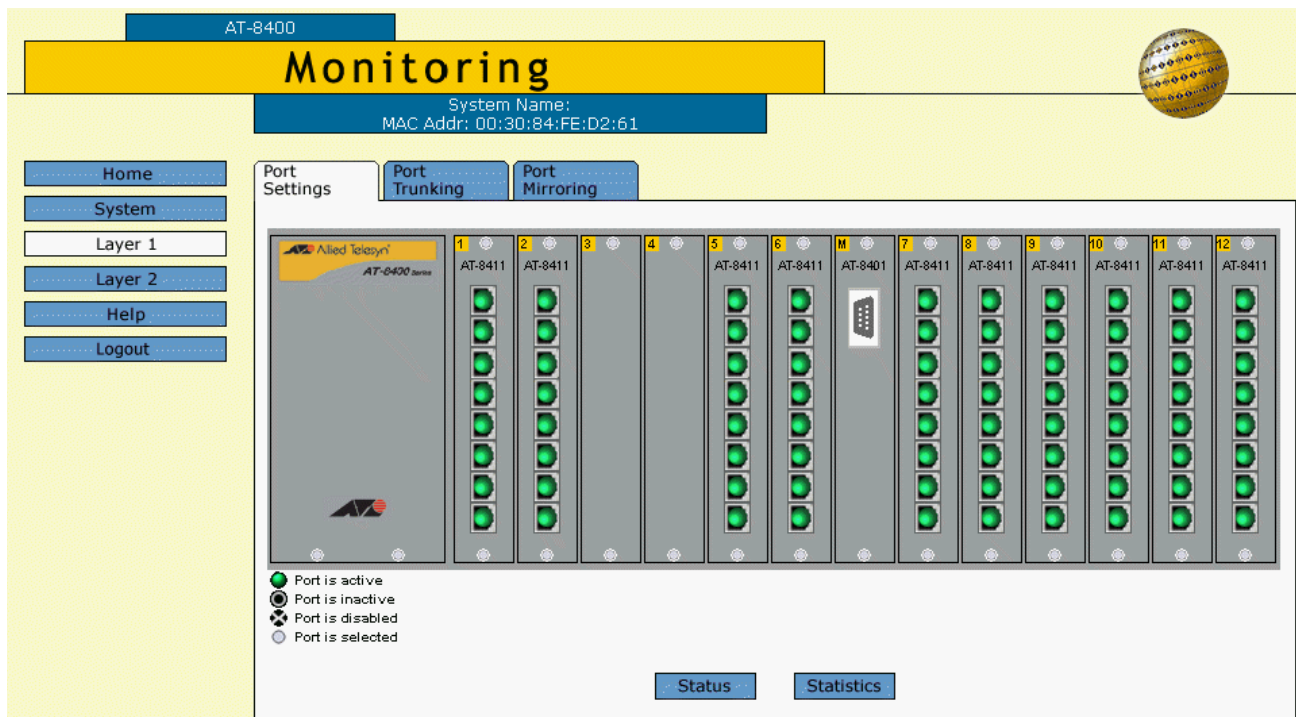


Figure 94 Port Monitoring Web Page

This page displays a graphical image of the front of the switch. Ports with a valid link to an end node are green.

4. Click on a port.

You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. After you select a port, it turns white. (To deselect a port, click it again.)

- Click **Status** to display the port's operating status or **Statistics** to display port statistics.

If you click **Status**, the Port Status Web Page is displayed as shown in Figure 95.

Port Status - Port(s) 3.1-8										
Total Ports Selected: 8. Page 1 of 1										
Port	Name	Link	Neg	MDIX	Speed	Duplex	PVID	Flow Ctl	STP State	Priority
3.1	Port_3.1	Up	Auto	MDIX	0100	Full	1	Disabled	Disabled	No
3.2	Port_3.2	Down	Auto	----	----	----	1	-----	Disabled	No
3.3	Port_3.3	Down	Auto	----	----	----	1	-----	Disabled	No
3.4	Port_3.4	Down	Auto	----	----	----	1	-----	Disabled	No
3.5	Port_3.5	Down	Auto	----	----	----	1	-----	Disabled	No
3.6	Port_3.6	Down	Auto	----	----	----	1	-----	Disabled	No
3.7	Port_3.7	Down	Auto	----	----	----	1	-----	Disabled	No
3.8	Port_3.8	Down	Auto	----	----	----	1	-----	Disabled	No

Figure 95 Port Status Web Page

The information in this window is for viewing purposes only. To adjust port parameters, refer to **Configuring Port Parameters** on page 271.

The columns in the window are described below:

Port

Indicates the port number in the following format:

slot number. port number

Name

Indicates the name of the port. The default name is the port number.

Link

The status of the link between the port and the end node connected to the port. Possible values are:

- ☐ Up - indicates that a valid link exists between the port and the end node.
- ☐ Down - indicates that the port and the end node have not established a valid link.

Neg

The status of Auto-Negotiation on the port. Possible values are:

- ☐ Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.
- ☐ Manual - Indicates that the operating speed and duplex mode have been set manually.

MDI/X

The operating configuration of the port. Possible values are Auto, MDI, MDI-X. The status Auto indicates that the port is automatically determining the appropriate MDI or MDI-X setting.

Speed

The operating speed of the port. Depending on the port you specified, possible values are:

- ☐ 0010 - Indicates 10 Mbps.
- ☐ 0100 - Indicates 100 Mbps.
- ☐ 1000 - Indicates 1000 Mbps.

Duplex

The duplex mode of the port. Possible values are half-duplex and full-duplex.

PVID

The port VLAN identifier currently assigned to the port.

Flow Control

The flow control setting for the port. Possible values are:

- ☐ Disabled - No flow control occurs on the port.
- ☐ Enabled - Flow control occurs on the port.

STP State

The current operating status of the port. Possible values are:

- ☐ Forwarding - The port is sending and receiving Ethernet frames. This is the normal state for a switch port.
- ☐ Disabled - STP operations have been disabled on the port.
- ☐ Blocking - This is the standby mode. The port does not participate in frame relay. The forwarding process discards received frames and does not submit forwarded frames for transmission.
- ☐ Listening - The port is enabled for receiving frames only. The port is preparing to participate in frame relay.
- ☐ Learning - The port is enabled for receiving frames only. The learning process can add new source address information to the forwarding database.

Priority

The priority assigned to packets that are received by the port. Possible values are:

- ☐ No - Indicates no override priority has been assigned to the port. Untagged packets are forwarded to the low priority queue. Tagged packets are forwarded to either the high or low queue, depending on the priority embedded in the packets.
- ☐ Low - Indicates low priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the low priority queue.
- ☐ High - Indicates high priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the high priority queue.

For more information, see **Class of Service Overview** on page 213.

Displaying Port Statistics

To display the statistics of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring page, select **Layer 1** from the sidebar.
Select the **Port Settings** tab. The Port Monitoring Web Page is shown in Figure 94 on page 276.
3. Select **Statistics**.
4. Click on a port.

You can select only one port when displaying statistics. After you select a port, it turns white. (To deselect a port, click it again.)

The Port Statistics Web Page is displayed in Figure 96.

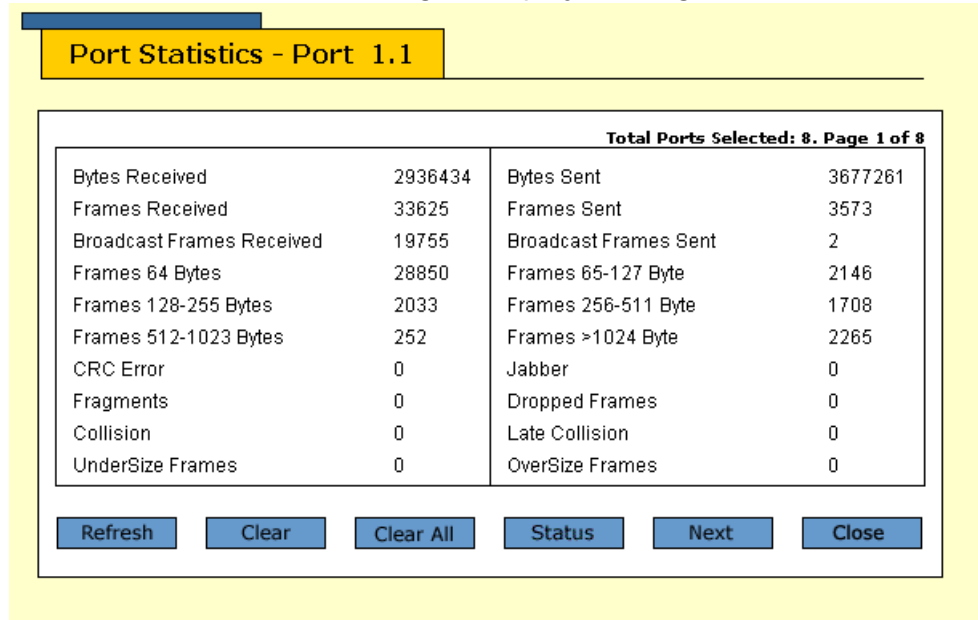


Figure 96 Port Statistics Web Page

The information in this window is for viewing purposes only. The statistics are defined below:

Bytes Received

Number of bytes received on the port.

Frames Received

Number of frames received on the port.

Broadcast Frames Received

Number of broadcast frames received on the port.

Frames 64 Bytes

Frames 128-255 Bytes

Frames 512-1023 Bytes

Number of frames transmitted from the port, grouped by size.

CRC Error

Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received on the port.

Fragments

Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received on the port.

Collision

Number of collisions that have occurred on the port.

Undersize Frames

Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received on the port.

Bytes Sent

Number of bytes transmitted from the port.

Frames Sent

Number of frames transmitted from the port.

Broadcast Frames Sent

Number of broadcast frames transmitted from the port.

Frames 65 - 127 Bytes**Frames 256 - 511 Bytes****Frames > 1024 Bytes**

Number of frames transmitted from the port, grouped by size.

Jabber

Number of received packets in which the packet data is greater than MAXFRAME SIZE and the packet has an invalid CRC.

Dropped Frames

Number of frames successfully received and buffered by the port, but discarded and not forwarded.

Late Collision

Number of received packets in which a late collision event has been detected.

Oversize Frames

Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received on the port.

Click **Clear** to clear the port statistics information for the port on the current page.

Click **Clear All** to clear the port statistics information for all the ports listed at the top of the Statistics Web Page.

Chapter 20

Port Security

This chapter explain how to display the port security status using a web browser management session. It contains the following procedure:

- ❑ **Displaying the Port Security Level** on page 283

Note

For background information on port security, refer to **Port Security Overview** on page 86.

Note

Port security cannot be set from a web browser management session. To set port security, use a local or Telnet management session.

Displaying the Port Security Level

To display the switch's port security levels, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Port Security** tab.

A graphical image that reflects the line cards installed in your chassis is displayed on the Port Security Web Page. See Figure 97.

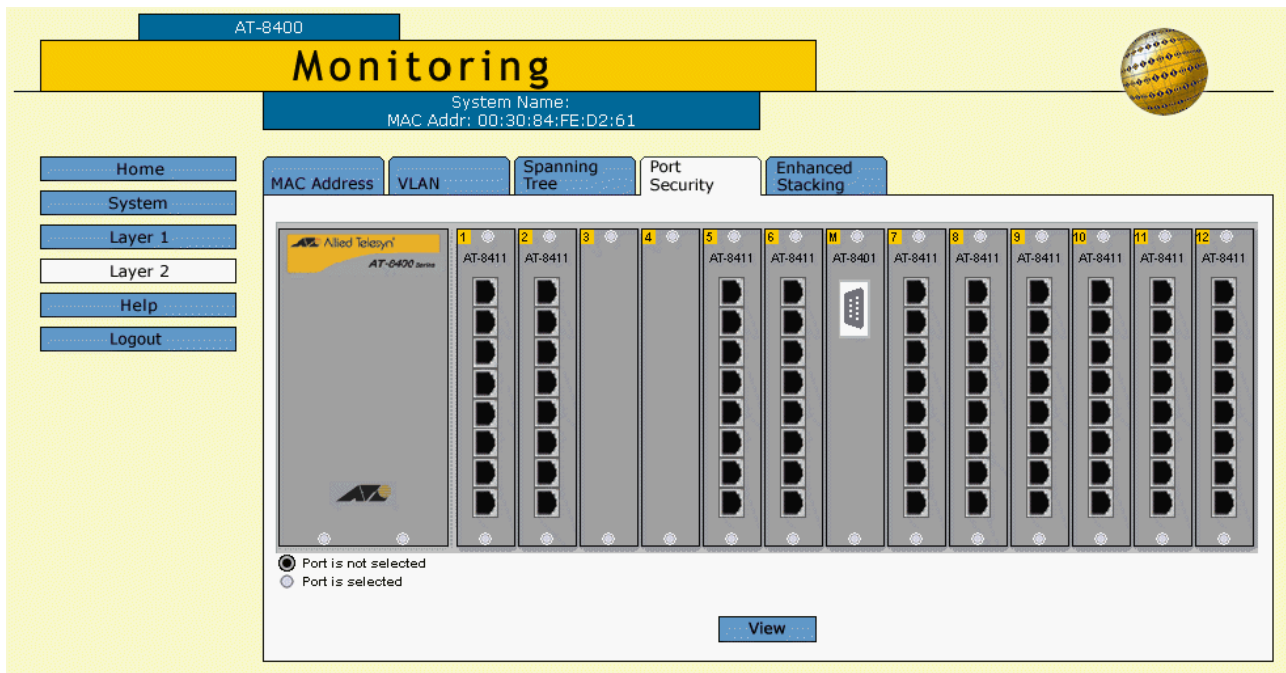


Figure 97 Port Security Web Page

4. Click on the ports to display their security status.

After you click on a port, it turns white. You can select multiple ports to display. (To deselect a port, click it again.)

5. Click **View**.

The Security for Ports Web Page appears as shown in Figure 98. This page displays the current security levels of the ports you selected.

Security for Port(s) - 2.1-8,8.1-8

Total Ports Selected: 16. Page 1 of 2

Port	Security Mode	Intruder Action	Participating	MAC Limit
2.1	Automatic	Discard	No	No Limit
2.2	Automatic	Discard	No	No Limit
2.3	Automatic	Discard	No	No Limit
2.4	Automatic	Discard	No	No Limit
2.5	Automatic	Discard	No	No Limit
2.6	Automatic	Discard	No	No Limit
2.7	Automatic	Discard	No	No Limit
2.8	Automatic	Discard	No	No Limit
8.1	Automatic	Discard	No	No Limit
8.2	Automatic	Discard	No	No Limit

Figure 98 Security for Ports Web Page

6. Here is a description of the headings that appear in the Security for Ports Web Page:

Port

Identifies the port in the AT-8400 switch in the following format:
slot number of line card. port number

Security Mode

There are four levels of port security:

- ☐ **Automatic:** The Automatic security mode disables port security. It is the default security level for the ports.
- ☐ **Limited:** You can use the Limited security level to manually specify a maximum number of dynamic MAC addresses that each port can learn.
- ☐ **Secured:** The Secured security level instructs a port to forward frames based solely on its static MAC address.

- ☐ **Lock all ports:** The Lock All Ports security level causes the switch to immediately stop learning new dynamic MAC addresses on behalf of the specified port.

For detailed information about the security mode parameter, see **Port Security Overview** on page 86.

Intruder Action

Indicates the action taken by the port if the security on the port is violated. Violating actions differ depending on the security level, as described below:

- ☐ **Limited** - The port receives a frame with a new source MAC address after the port has learned its maximum number of dynamic MAC addresses.
- ☐ **Secured** - The port receives a frame with a MAC address that has not been entered as a static address on the port.
- ☐ **Locked** - The port receives a frame with a new source MAC address.

You can configure the port to take one of the following intrusion actions if a violating event occurs:

- ☐ **Discard** - Discards the invalid frame.
- ☐ **Trap** - Discards the invalid frame and sends a trap to a management workstation.
- ☐ **Disable** - Discards the invalid frame, sends a trap to a management workstation, and disables the port.

Participating

Indicates the port is participating in port security.

MAC Limit

Indicates the maximum number of dynamic MAC addresses the port can learn when it is operating under the Limited security level.

Chapter 21

Port Trunks

This chapter explains how to configure a port trunk using a web browser management session.

This chapter contains the following procedures:

- ❑ **Creating or Deleting a Port Trunk** on page 287
- ❑ **Modifying a Port Trunk** on page 290

Note

For background information on port trunking, refer to **Port Trunking Overview** on page 93.

Creating or Deleting a Port Trunk

The following procedures allow you to create or delete a port trunk using the web browser management session. After you have made your changes, return to **System** on the sidebar and select **Save Changes**.

Creating a Port Trunk

To create a port trunk, perform the following procedure:



Caution

Configure the software for ports on the switch and the end node before you connect the cables of a port trunk. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms. This can adversely effect the operations of your network.

1. From the Home page, select **Configuration**.

The Configuration System Web Page is displayed. See Figure 82 on page 248.

2. From the Configuration page, select **Layer 1**.

The Port Settings Web Page is displayed. See Figure 92 on page 271.

3. Select the **Port Trunking** tab.

The Port Trunking Web Page is displayed in Figure 99.

AT-8400

Configuration

System Name: Middle School
MAC Addr: 00:30:84:EE:31:08

Home System **Layer 1** Layer 2 Help

Port Settings **Port Trunking** Port Mirroring

Total Trunks : 2. Page 1 of 1

ID	Name	Type	Ports
1	highschool	10/100MB	1,2-4
2	elementaryschool	10/100MB	4,1-2

Refresh Modify Remove Add

Figure 99 Port Trunk Web Page

4. Click **Add**.

The Add New Trunk Web Page is displayed in Figure 100.

Add New Trunk

Trunk ID

Trunk Name

Trunk Type ☒ 10/100 ☐ Gigabit

1 AT-8411 2 AT-8411 3 AT-8411 4 AT-8401 5 AT-8411 6 AT-8411 7 AT-8411 8 AT-8411 9 AT-8411 10 AT-8411 11 AT-8411 12 AT-8411

☐ Trunk Port
☒ Regular Port

Apply Cancel

Figure 100 Add New Trunk Web Page

5. Enter the name of the trunk in the Trunk Name box.
6. Click on the ports you want to include in the trunk.
Selected ports turn white. To deselect a port, click it again.
7. Scroll down the Web Page.
8. Click **Apply**.

You are returned to the Port Trunking Web Page. It is updated with the new trunk port information. The new port trunk is immediately activated on the switch.

9. Click **System** on the sidebar.
The Configuration Web Page appears.
10. Click **Save Changes** at the bottom of the web page.
Your changes are saved on the switch.

11. Configure the ports on the remote switch for port trunking.

You can now connect the data cables to the ports of the trunk on the switch.

Deleting a Port Trunk

To delete a port trunk, perform the following procedure.



Caution

Before you delete a trunk in software, disconnect the cables from the ports. Deleting the trunk without disconnecting the data cables can create a loop in your network topology. This can result in broadcast storms.

1. From the Home page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. From the Configuration page, select **Layer 1**.
The Port Settings Web Page is displayed. See Figure 92 on page 271.
3. Select the **Port Trunking** tab.
The Port Trunking Web Page is displayed in Figure 99 on page 287.
4. Select a trunk from the Port Trunking Web Page.
A green light appears next to the selected trunk.
5. Click **Remove**.
The port is deleted from the switch. The Port Trunking Web Page is updated to reflect your changes.
6. Click **System** on the sidebar.
The Configuration Web Page appears.
7. Click **Save Changes** at the bottom of the web page.
Your changes are saved on the switch.

Modifying a Port Trunk

This procedure allows you to modify a port trunk using a web browser management session.

To modify a port trunk, perform the following procedure:

1. From the Home page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. From the Configuration page, select **Layer 1**.
The Port Settings Web Page is displayed. See Figure 92 on page 271.
3. Select the **Port Trunking** tab.
The Port Trunking Web Page is displayed in Figure 99 on page 287.
4. Select **Modify**.

The Modify Trunk Web Page is shown in Figure 101.

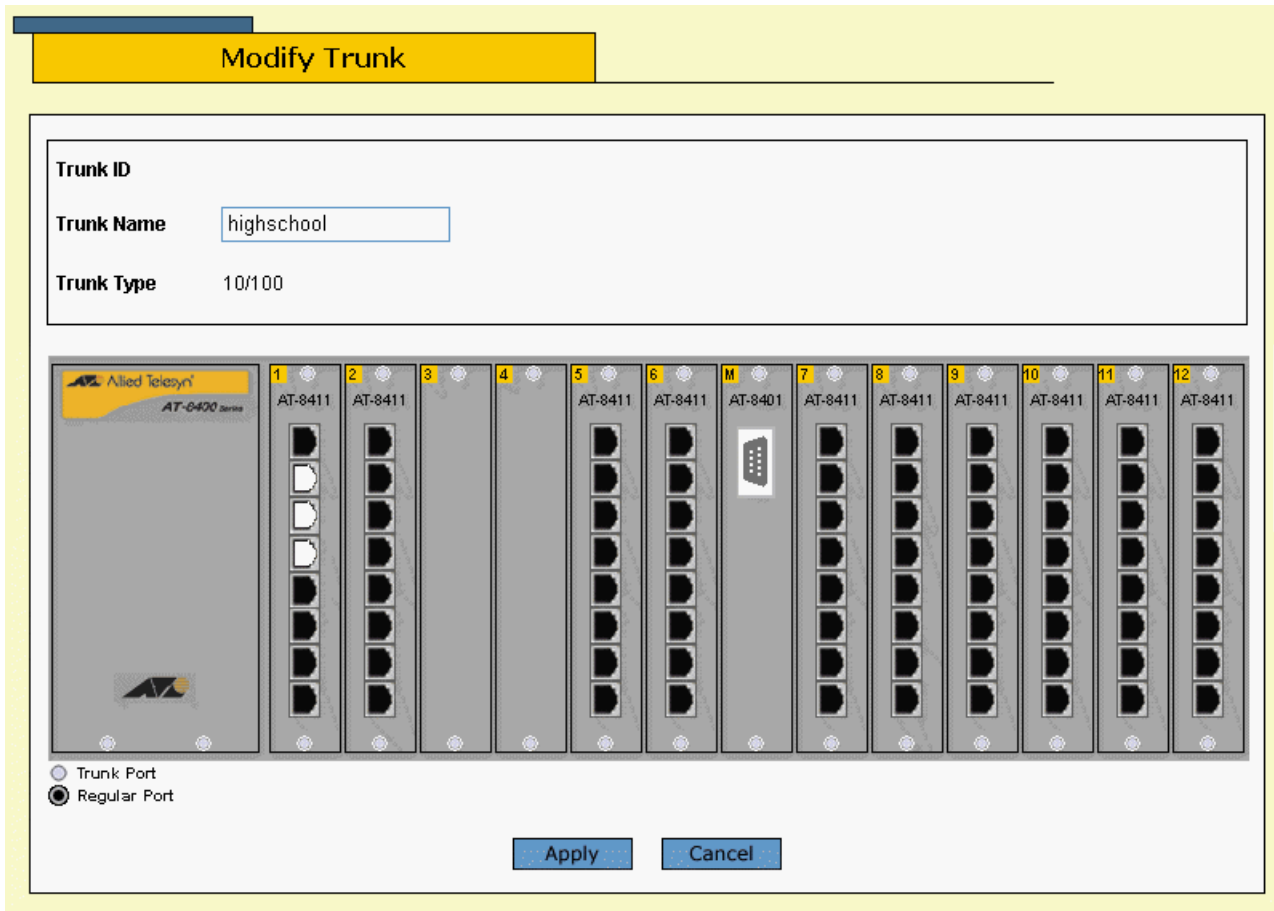


Figure 101 Modify Trunk Web Page

- Click on the ports to select them for port trunking.
Selected ports turn white. Click again to deselect a port.
- Click **Apply**.
- The Port Trunking Web Page appears as shown in Figure 99 on page 287.
Your changes are immediately activated on the switch.
- Click **System** from the sidebar.
The Configuration Web Page is displayed.
- Click **Save Changes**.
The port trunk you modified is saved on the switch.

Chapter 22

Port Mirroring

This chapter explains how to configure a port mirror using a web browser management session.

This chapter contains the following procedures:

- ❑ **Creating a Port Mirror** on page 293
- ❑ **Deleting a Port Mirror** on page 295
- ❑ **Modifying a Port Mirror** on page 295

Note

For background information on port mirroring, refer to **Port Mirroring Overview** on page 108.

Creating or Deleting a Port Mirror

Use the following procedures to create, delete, or modify a port mirror. For information about how ports are specified, see **Specifying Ports** on page 26. After you have made your changes, you need to save them on the Configuration System Web Page.

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the Home Page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. From the Configuration page, select **Layer 1** from the sidebar.
The Port Settings Web Page is displayed. See Figure 92 on page 271.
3. Select the **Port Mirroring** tab.
The Port Mirroring Web Page is displayed as shown in Figure 102.

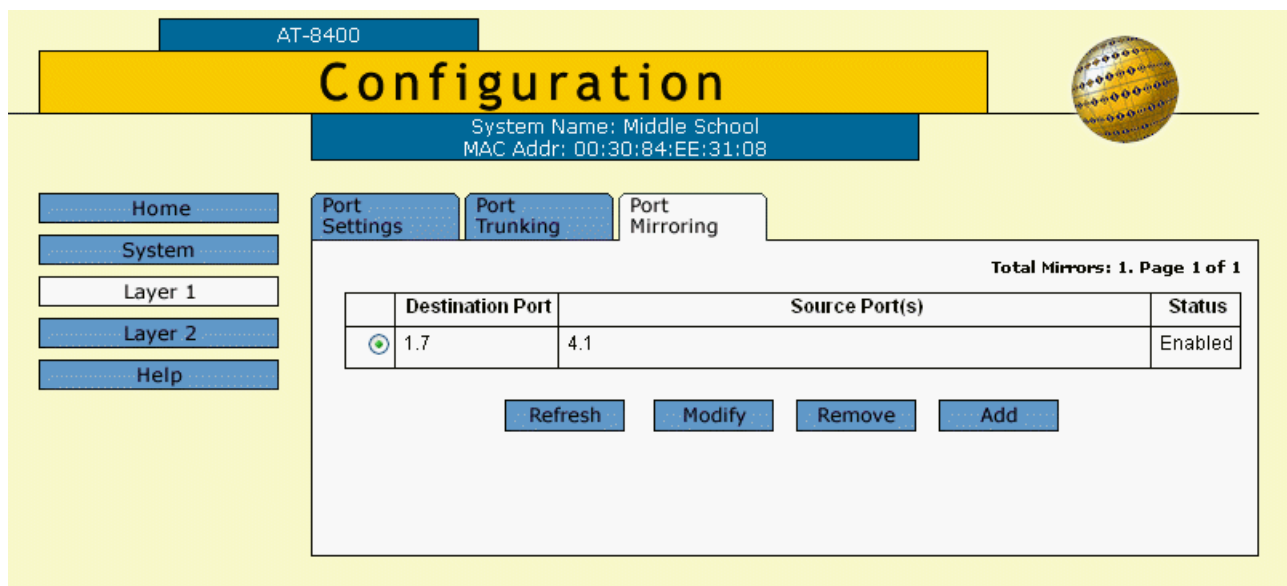


Figure 102 Port Mirroring Web Page

4. To create a port mirror, do the following.
5. Click **Add**.

The Add New Mirror Web Page is displayed as shown in Figure 103 on page 294.

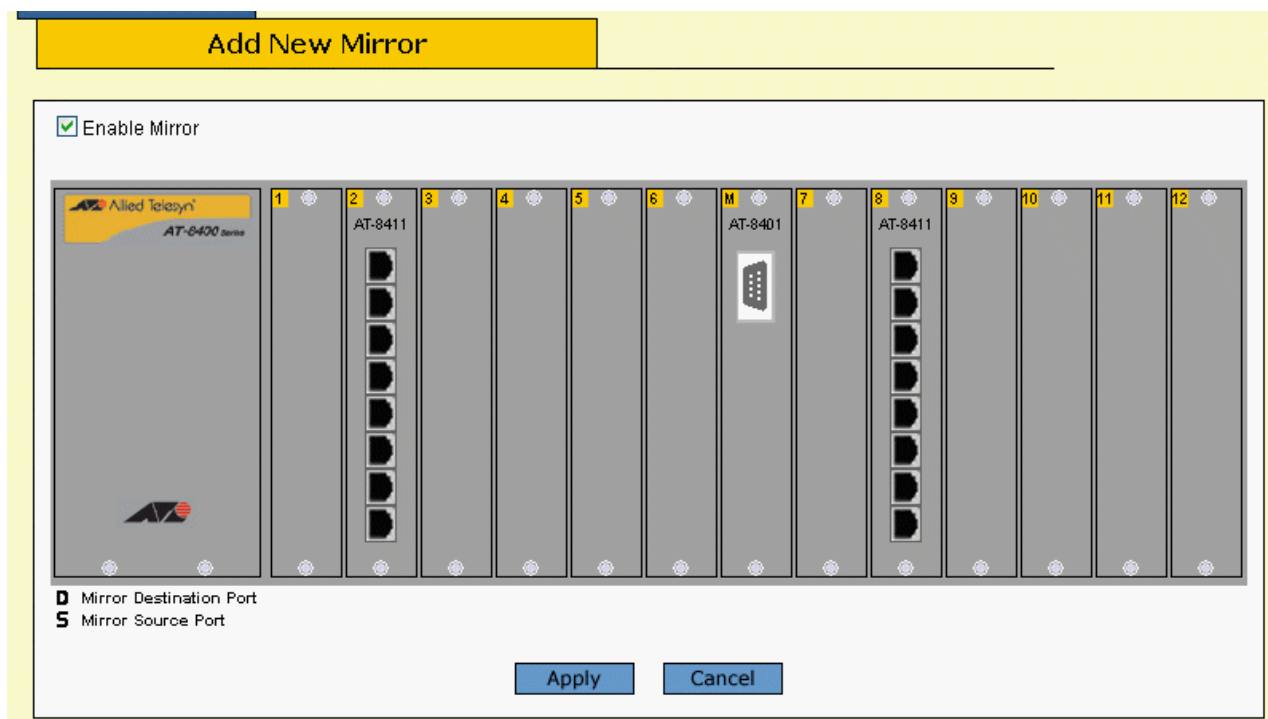


Figure 103 Add New Mirror Web Page

6. Click the ports in the graphical switch image.
Click once for S which stands for the source mirror port. Click twice for D which stands for destination mirror port. Click three times to deselect a port.
7. Click **Apply**.
The Port Mirroring Web Page is displayed. It reflects the changes you made in Step 6. The port mirror is immediately activated on the switch.
8. Select **System** from the sidebar.
The Configuration Web Page is displayed.
9. Click **Save Changes**.
You can connect a data analyzer to the destination mirror port to monitor the traffic on the selected ports.

Deleting a Port Mirror

Use this procedure to delete a port mirror using a web browser management session.

1. From the Home Page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. From the Configuration page, select **Layer 1** from the sidebar.
The Port Settings Web Page is displayed. See Figure 92 on page 271.
3. Select the **Port Mirroring** tab.
The Port Mirroring Web Page is displayed as shown in Figure 102.
4. Click on the port mirror you want to remove.
The circle next to the port mirror turns green.
5. Click **Remove** to delete a port mirror.
The port mirror is deleted. The Port Mirroring Web Page is updated to reflect your changes.
6. Select **System** from the sidebar.
The Configuration Web Page is displayed.
7. From the Configuration Web Page, click **Save Changes**.
You can now use the port that was functioning as the destination mirror port for normal network operations.

Modifying a Port Mirror

To change the source mirror port or the destination mirror port on an existing port mirror, perform the following procedure.

1. From the Home Page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. From the Configuration page, select **Layer 1** from the sidebar.
The Port Settings Web Page is displayed. See Figure 92 on page 271.
3. Select the **Port Mirroring** tab.
The Port Mirroring Web Page is displayed as shown in Figure 102.
4. Click **Modify** to modify a port mirror.

The Modify Web Page is displayed as shown in Figure 104.

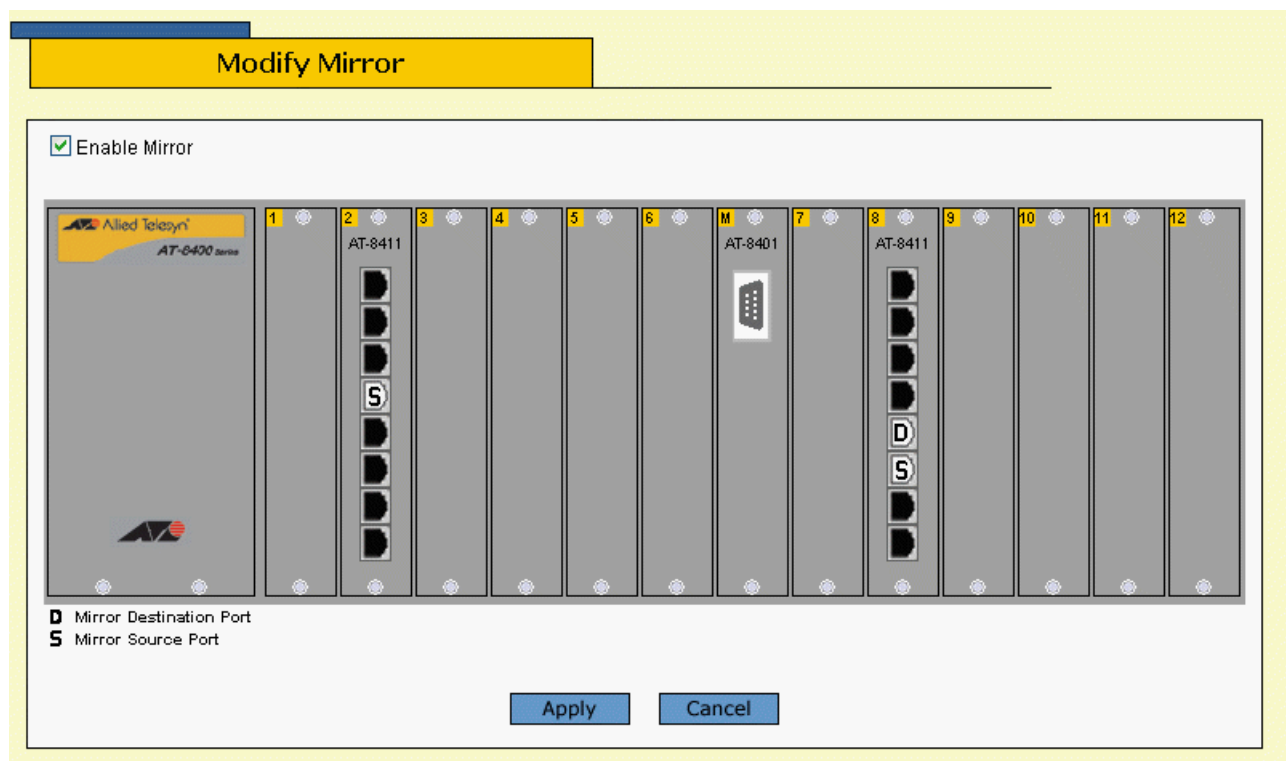


Figure 104 Modify Mirror Web Page

5. Make your changes to the mirror ports.

Click once to select **S** - source mirror port. To change your **D** - destination mirror port, you must deselect your current destination port mirror by clicking it off. Then you can click on a new destination port mirror.

6. Click **Apply**.

Your changes are activated on the switch. The Port Mirroring Web Page appears with the new ports.

7. Select **System** from the sidebar.

The Configuration System Web Page is displayed.

8. Select **Save Changes**.

Your modifications to the port mirror or port mirrors are saved to the switch.

Chapter 23

STP, RSTP, and MSTP

This chapter explains how to configure STP, RSTP, and MSTP parameters on an AT-8400 chassis using a web browser management session. It contains the following procedures:

- ❑ **Activating STP, RSTP, or MSTP** on page 298
- ❑ **Configuring STP** on page 300
- ❑ **Configuring RSTP** on page 304
- ❑ **Configuring MSTP** on page 309
- ❑ **Displaying STP, RSTP, or MSTP Settings** on page 317

Note

For background information on STP and RSTP, refer to **STP and RSTP Overview** on page 117. For background information on MSTP, refer to **MSTP Overview** on page 141.

Activating STP, RSTP, or MSTP

The AT-8400 Series switch can support the three spanning tree protocols STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. So before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol. Once selected, you can then enable or disable it.

To select the active spanning tree protocol and to enable or disable it, perform the following procedure:

Note

Changing the active spanning tree protocol resets the switch.

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

The Spanning Tree Web Page appears as shown in Figure 105.

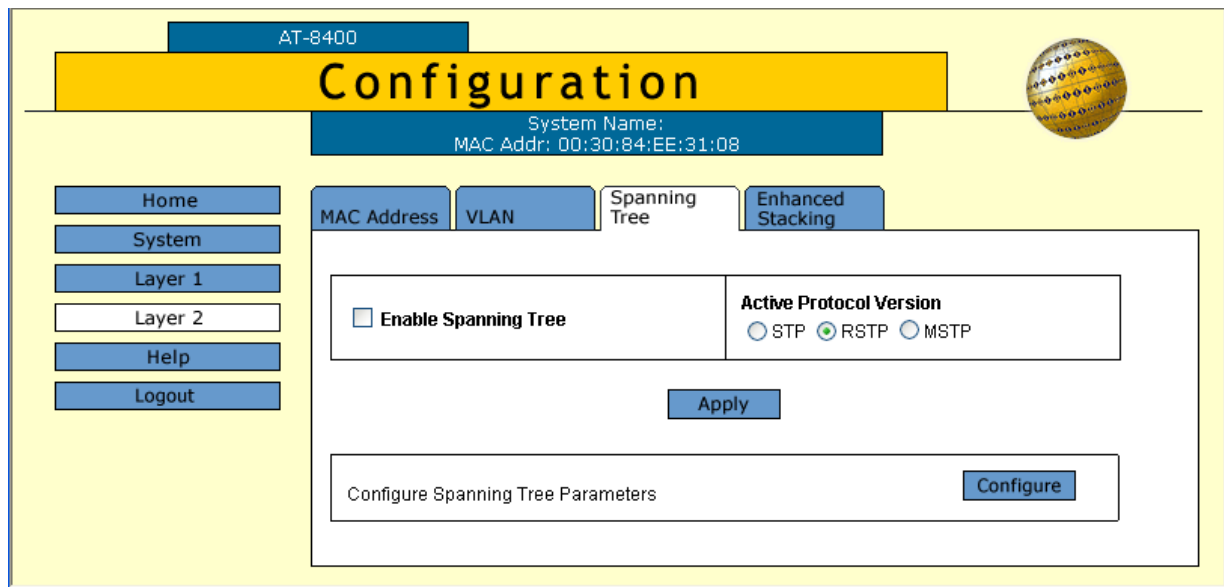


Figure 105 Spanning Tree Web Page

Note

If you do not want to change the active spanning tree protocol and just want to enable or disable it, go to Step 5.

4. To change the active spanning tree protocol on the switch, click **STP**, **RSTP**, or **MSTP** in the Active Protocol Version section of the window. The default is RSTP.

Note

Only one spanning tree protocol can be active on the switch at a time.

5. To enable or disable the active spanning tree protocol on the switch, click the **Enable Spanning Tree** check box. A check indicates that the spanning tree is enabled while no check indicates that spanning tree is disabled. The default is disabled.
6. Click **Apply**.

Note

If you changed the active spanning tree protocol, the switch resets and your management session is ended. To continue managing the switch, you must restart your management session after the switch is finished reloading the AT-S60 management software.

7. If you activated STP, go to **Configuring STP** on page 300. If you activated RSTP go to **Configuring RSTP** on page 304. If you activated MSTP, go to **Configuring MSTP** on page 309.

Configuring STP

To configure STP, perform the following procedure:



Caution

The bridge provides default STP parameters that are adequate for most networks. Changing the STP parameters without prior experience and an understanding of how STP works may have a negative effect on your network. Consult the IEEE 802.1d standard before changing any of the STP parameters.

1. Follow the steps in the procedure described in **Activating STP, RSTP, or MSTP** on page 298, then select STP as your active protocol version.
2. Click **Configure**.

The Spanning Tree Expanded Web Page is displayed as shown in Figure 106.

AT-8400

Configuration

System Name:
MAC Addr: 00:30:84:FE:D2:61

Home System Layer 1 Layer 2 Help Logout

MAC Address VLAN Spanning Tree Enhanced Stacking

Configure STP Parameters

Bridge Priority [0-15] 8 * 4096 = 32768 Bridge Hello Time [1-10] 2 Bridge Forwarding [4-30] 15	Bridge Max Age [6-40] 20 Bridge Identifier 00:30:84:FE:D2:61
--	---

Apply Defaults

Port	1	2	3	4	5	6	M	7	8	9	10	11	12
AT-8411	AT-8411	AT-8411			AT-8411	AT-8411	AT-8401	AT-8411	AT-8411	AT-8411	AT-8411	AT-8411	AT-8411

☒ Port is not selected
☐ Port is selected

Modify Back

Figure 106 Spanning Tree Expanded Web Page

- Adjust the bridge STP settings as needed. The parameters are described below.

Enable Spanning Tree

To enable or disable spanning tree, click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.

Force Version

This parameter displays the version active on the switch. Click on the circle next to the Force STP Compatible or RSTP.

Bridge Priority

The priority number for the AT-8401 management card. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 15, with 0 having the highest priority.

Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding

The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have adapted to the change, possibly resulting in a network loop. You can set this parameter from 4 to 30 seconds. The default is 30 seconds.

Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. You can set this parameter from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, you **must** observed the following equations:

$$\text{MaxAge} < (2 \times (\text{HelloTime} + 1))$$

$$\text{MaxAge} < (2 \times (\text{ForwardingDelay} - 1))$$

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

4. After you have made the desired changes, click **Apply**.
If you are finished making changes, skip to step 9.
5. To adjust a port's STP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

The STP Settings Web Page is displayed in Figure 107.

Figure 107 STP Settings Web Page

6. Adjust the settings as desired. The parameters are described below.

Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The default value for priority is 128. The range is 0-15, with 0 having the highest priority.

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. Enter a value from 0 to 200,000,00. The default values are:

- ☐ 0 for Auto-detect
- ☐ 4 for a 1 Gigabit port
- ☐ 10 for a 10 Mbps port
- ☐ 100 for a 100 Mbps port

7. Once you have configured the parameters, click **Apply**.
8. Click **System** from the sidebar.

The Configuration Web Page is displayed.

9. Click **Save Changes** at the bottom of the web page.

The changes you made are saved on the switch.

Configuring RSTP

To configure RSTP, perform the following procedure.



Caution

The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. Consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. Follow the steps in the procedure described in **Activating STP, RSTP, or MSTP** on page 298.
2. Select RSTP as your active protocol version.
3. Click **Configure**.

The Configure RSTP Parameters Web Page is displayed as shown in Figure 108.

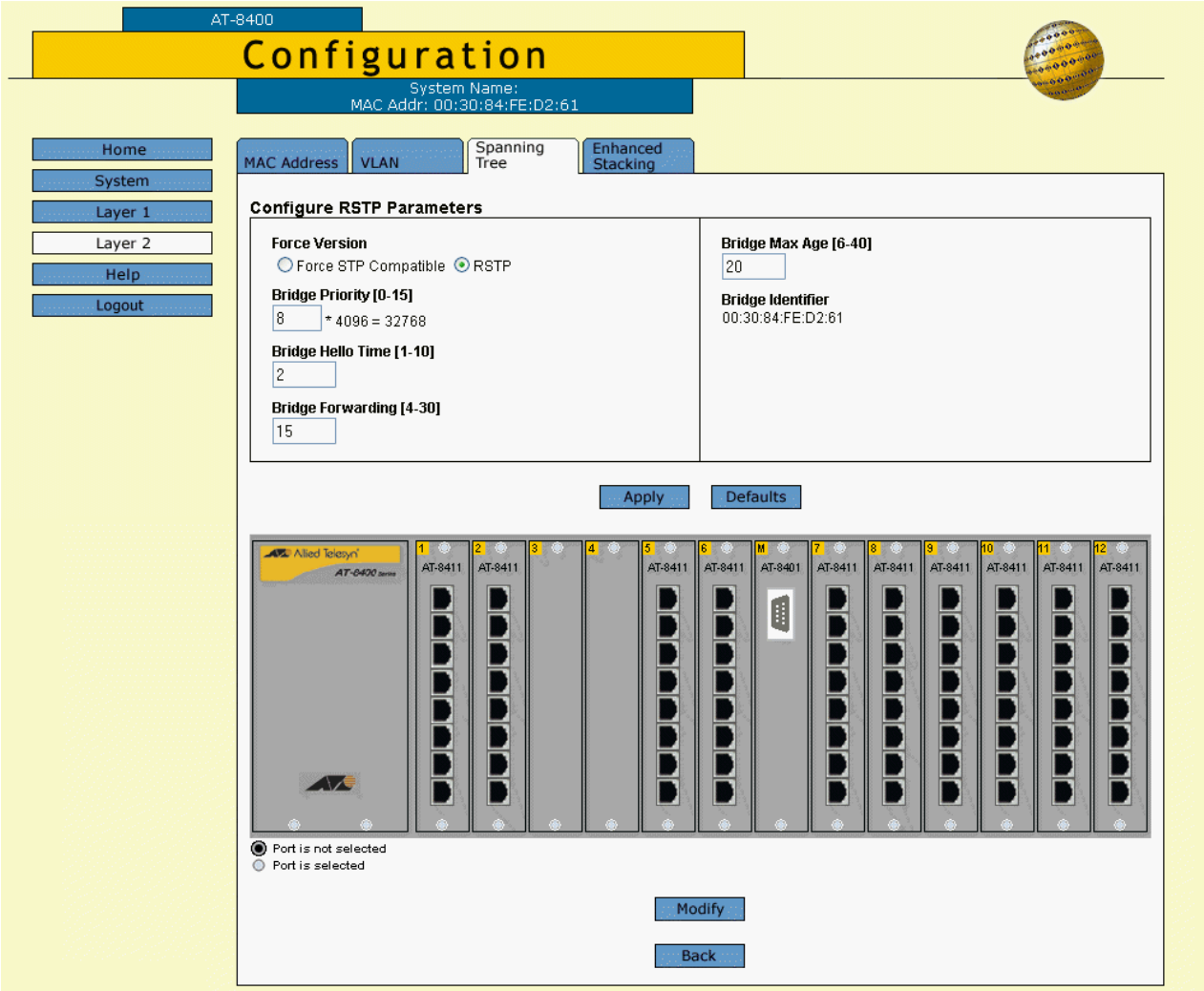


Figure 108 Configure RSTP Parameters

4. Adjust the parameters as desired. The parameters are defined below.

Force Version

This selection determines whether the bridge will operate with RSTP or in an STP-compatible mode. The default is RSTP. If you select RSTP, the bridge operates all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge operates all ports in STP.

Bridge Priority

The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 15, with 0 having the highest priority. For a list of the increments, refer to **Table 1, Bridge Priority Value Increments** on page 119

Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

Bridge Forwarding

The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds.

Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, you **must** observe the following equations:

$$\text{MaxAge} < (2 \times (\text{HelloTime} + 1))$$

$$\text{MaxAge} < (2 \times (\text{ForwardingDelay} - 1))$$

Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

5. After you have made your changes, click **Apply**.
6. To adjust a port's RSTP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

The RSTP Settings Web Page is displayed as shown in Figure 109.

RSTP Settings - Port(s) 1.2	
Port Priority [0-15] <input type="text" value="8"/> * 16 = 128 Path Cost [0 - 200000000] <input type="text" value="0"/> (0 = Auto Update)	Point-To-Point <input type="button" value="Auto Detect"/> ▾ Edge Port <input type="button" value="Yes"/> ▾
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 109 RSTP Settings Web Page

7. Adjust the settings as desired. The parameters are described below.

Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value of 128). For a list of the increments, refer to **Table 4, Port Priority Value Increments** on page 121.

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for the specified LAN. The range is 0 to 200,000,000.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. The default setting is Auto-detect, which sets port

cost depending on the speed of the port. Default values are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

Edge Port

This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

8. Once you have configured the parameters, click **Apply**.
9. Click **System** from the sidebar.
The Configuration Web Page is displayed.
10. Click **Save Changes** at the bottom of the web page.
The changes you made are saved on the switch.

Configuring MSTP

This section is divided into the following procedures:

- ❑ **Configuring MSTP and CIST Parameters** on page 309
- ❑ **Associating VLANs to MSTIs** on page 312
- ❑ **Configuring MSTP Port Parameters** on page 315

Note

MSTP must be selected as the active spanning tree protocol on the switch before you can configure it. For instructions on selecting the active spanning tree, refer to **Activating STP, RSTP, or MSTP** on page 298.

Configuring MSTP and CIST Parameters

To configure MSTP parameters, perform the following procedure:

1. From the Home page, select **Configuration**.
2. From the Configuration page, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

The Spanning Tree Web Page appears as shown in Figure 105 on page 298.

4. Click the **Configure** button.

The MSTP Spanning Tree Expanded Web Page is displayed as shown in Figure 110.

AT-8400

Configuration

System Name:
MAC Addr: 00:30:84:FE:D2:61

Home

System

Layer 1

Layer 2

Help

Logout

MAC Address

VLAN

Spanning Tree

Enhanced Stacking

Configure MSTP Parameters

Force Version

☐ Force STP Compatible

☒ MSTP

Bridge Hello Time [1-10]

2

Bridge Forwarding [4-30]

15

Configuration Name

Bridge Max Age [6-40]

20

Bridge Max Hops [1-40]

20

Revision Level [0-255]

0

Apply

Defaults

Configure CIST Parameters

CIST Priority [0-15]

8

* 4096 = 32768

Apply

CIST/MSTI Table

Total CIST/MSTIs: 1. Page 1 of 1

	CIST/MSTI ID	Priority	VLAN Associations
<input checked="" type="radio"/>	0	32768	1

Refresh

Add

AT-8411

AT-8411

AT-8411

AT-8411

AT-8401

AT-8411

AT-8411

AT-8411

AT-8411

AT-8411

AT-8411

Port is not selected

Port is selected

Modify

Back

Figure 110 MSTP Spanning Tree Expanded Web Page

310

Note

This procedure explains the Configure MSTP Parameters and Configure CIST Parameters sections of the web page. The CIST/MSTI Table is explained in **Associating VLANs to MSTIs** on page 312. The graphic image of the switch is described in **Configuring MSTP Port Parameters** on page 315.

5. Adjust the bridge MSTP settings as needed. The parameters are described below.

Force Version

This selection determines whether the bridge will operate with MSTP or in an STP-compatible mode. If you select MSTP, the bridge operates all ports in MSTP, except those ports that receive STP or RSTP BPDU packets. If you select Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. The default is MSTP.

Bridge Hello Time

The time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds. This value is active only if the bridge is selected as the root bridge of the network.

Bridge Forwarding

The waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all of the links may have adapted to the change, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Configuration Name

The name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters in length. The name, which is case-sensitive, must be the same on all bridges in a region. Examples of a configuration name include Sales Region and Production Region.

Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs.

All bridges in a single-instance bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be less than $(2 \times (\text{HelloTime} + 1))$

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

Bridge Max Hops

MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses an MSTP region boundary. Once the counter reaches zero, the BPDU is deleted.

Revision Level

The revision level of an MSTP region. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 255.

CIST Priority

The priority number for the bridge. This number is used in determining the root bridge of the bridged network. This number is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

6. Once you have adjusted the parameters, click the **Apply** button.

Associating VLANs to MSTIs

This section explains how to create and delete MSTI IDs and how to associate VLANs to MSTI IDs.

To manage the MSTI ID and VLAN associations, perform the following procedure:

1. Display the Spanning Tree Expanded Web Page for MSTP by performing Steps 1 through 4 in the procedure **Configuring MSTP and CIST Parameters** on page 309.

2. To create or delete an MSTI ID and to associate VLANs to MSTIs, do the following:
 - a. In the CIST/MSTI Table section of the menu, click **Add**.
The Add New MSTI Web Page is displayed as shown in Figure 111.

Figure 111 Add New MSTI Web Page

- b. In the MSTI ID field, enter a new MSTI ID. The range is 1 to 15.
 - c. In the Priority field, enter a MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. This parameter is used in selecting a regional root for the MSTI. For a list of the increments, refer to **Table 1, Bridge Priority Value Increments** on page 119. The default is 0.
 - d. In the VLAN List field, enter the VIDs of the VLANs to be associated with this MSTI. You can specify more than one VID at a time (e.g., 2,4,7).
 - e. Click **Apply**.
 - f. Repeat this procedure to create more MSTI IDs.
3. To add or remove VLANs or to change the MSTI Priority value of an existing MSTI ID, do the following:
 - a. In the CIST/MSTI Table section of the menu, click the circle next to the MSTI ID you want to modify. You can select only one MSTI ID at a time. You cannot modify CIST.
 - b. Click **Modify**.

The Modify MSTI Web Page is displayed as shown in Figure 112.

Modify MSTI

MSTI ID : 2

Priority : 7 * 4096 = 28672

VLAN List : 3

Apply Cancel

Figure 112 Modify MSTI Web Page

- c. In the Priority field, enter a new MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. For a list of the increments, refer to **Table 1, Bridge Priority Value Increments** on page 119. The default is 0.
- d. In the VLAN List field, modify the list of VIDs of the VLANs to be associated with this MSTI. You can add more VLANs or remove VLANs. You can specify more than one VID at a time (e.g., 2,4,7). If you remove a VLAN, the VLAN will be associated with CIST.
- e. Click **Apply**.
- f. Repeat this procedure to modify more MSTI IDs.
4. To delete an MSTI ID, do the following:
 - a. In the CIST/MSTI Table section of the menu, click the circle next to the MSTI ID you want to delete. You can select only one MSTI ID at a time.
 - b. Click **Remove**.
A confirmation prompt is displayed.
 - c. Click **OK** to delete the MSTI or **Cancel** to cancel the procedure.
If you select OK, the MSTI is deleted and VLANs associated with it are returned to CIST, which has an ID of 0.

Configuring MSTP Port Parameters

To configure MSTP port parameters, perform the following procedure:

1. Perform Steps 1 through 4 in the procedure **Configuring MSTP and CIST Parameters** on page 309 to display the Spanning Tree Expanded Web Page for MSTP.
2. In the diagram of the switch at the bottom of the MSTP Spanning Tree Expanded Web Page, click the ports you want to configure. You can select more than one port at a time.
3. Click **Configure**.

The Configure MSTP Port Settings Web Page is displayed as shown in Figure 113.

Figure 113 MSTP Port Settings Web Page

4. Adjust the parameters as needed. The parameters are described below.

Port Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value is 128). For a list of the increments, refer to **Table 4, Port Priority Value Increments** on page 121.

Port Internal Path Cost

The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Edge Port

This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to **Point-to-Point Ports and Edge Ports** on page 122.

Port External Path Cost

The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP. The range is 0 to 200,000,000. The default setting is 200,000.

5. After adjusting the parameters, click **Apply**.
6. Repeat this procedure to configure MSTP parameters for other switch ports.

Displaying STP, RSTP, or MSTP Settings

To display spanning tree parameter settings, perform the following procedure:

1. From the Home page, select **Monitoring**.
2. From the Monitoring menu, select **Layer 2**.
3. From the Layer 2 page, select the **Spanning Tree** tab.

The Monitoring Spanning Tree Web Page is displayed in Figure 115. This window displays whether spanning tree is enabled or disabled and which spanning tree protocol is active.

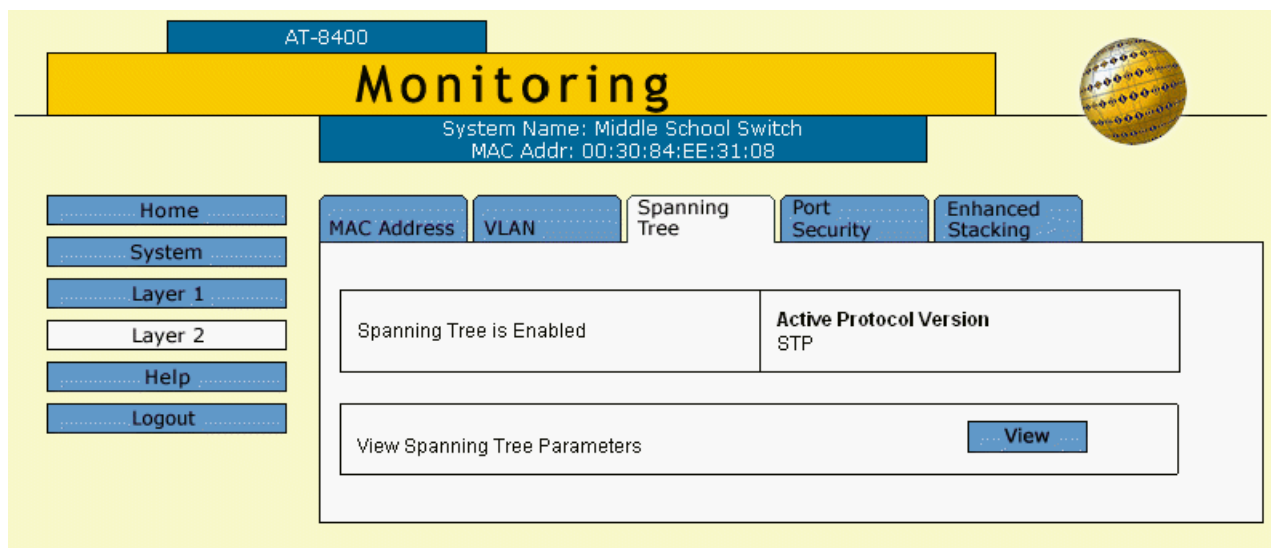


Figure 114 Monitoring Spanning Tree Web Page

4. To view the current settings for the active spanning tree protocol, click **View**.

Figure 115 shows an example of the Monitor STP Parameters Web Page. The contents of this window will differ depending on which spanning tree protocol is active on the switch. The information in this window is for viewing purposes only.

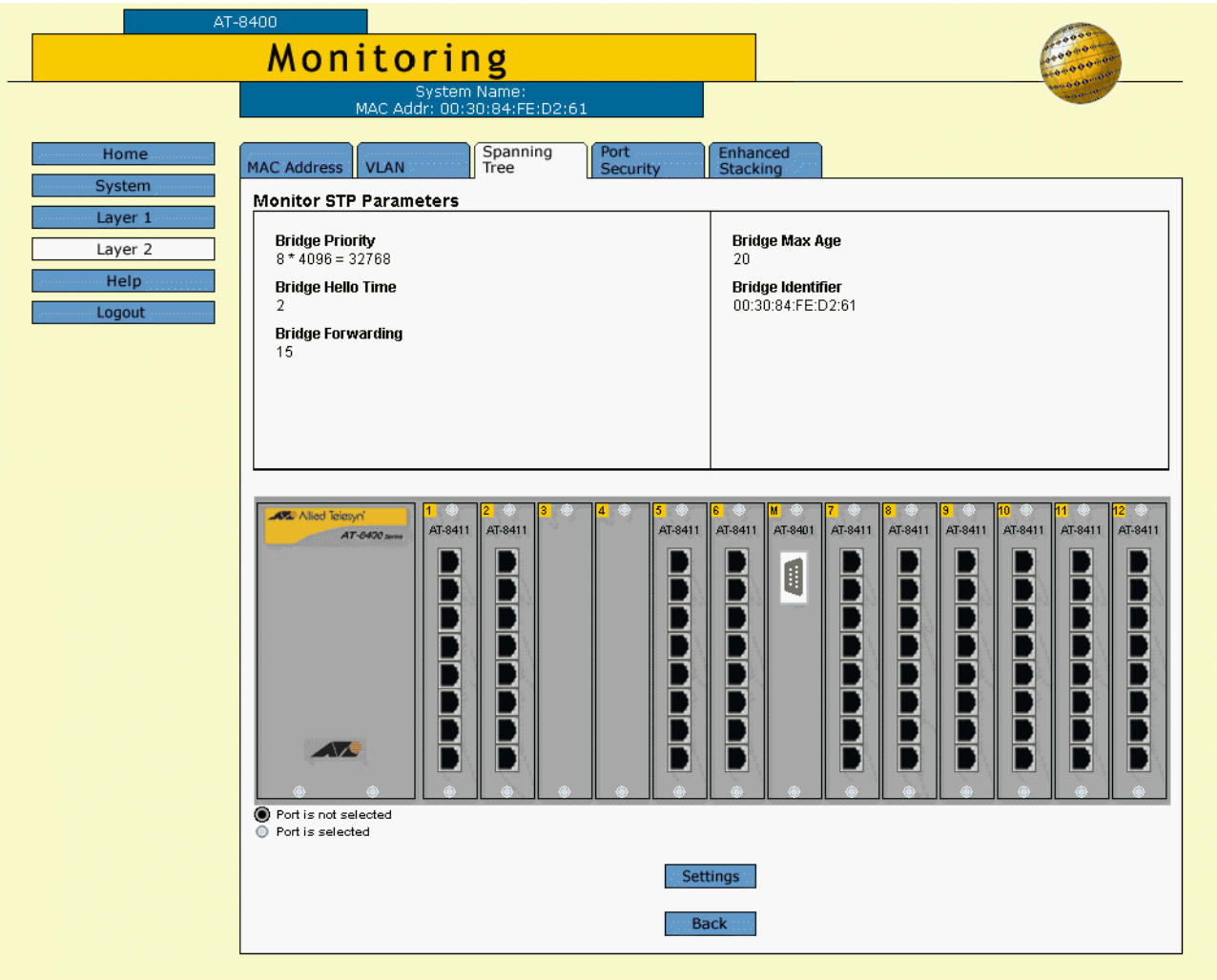


Figure 115 Monitor STP Parameters Web Page

5. To view port settings, click a port in the switch and click **Settings**. You can select more than one port.

The Monitor STP Settings Web Page appears as shown in Figure 116.

STP Settings - Port(s) 4.2-3

Total Ports Selected: 2. Page 1 of 1			
Port	State	Cost	Priority
4.2	Disabled	Auto Update	128
4.3	Disabled	Auto Update	128

OK

Figure 116 Monitor STP Settings Web Page

6. Click **OK**.

Chapter 24

Virtual LANs

This chapter explains how to create, modify, and delete VLANs using a web browser management session. In addition, this chapter explains how to change a switch's VLAN operating mode.

This chapter contains the following procedures:

- ❑ **Creating a VLAN** on page 321
- ❑ **Modifying a VLAN** on page 324
- ❑ **Deleting VLANs** on page 326
- ❑ **Displaying VLANs** on page 327
- ❑ **Setting the Switch's VLAN Mode** on page 328

Note

For background information on VLANs and on the Basic VLAN mode, refer to **Chapter 10, Virtual LANs**.

Creating a VLAN

To create a new port-based or tagged VLAN, perform the following procedure. Before you create a VLAN, you may want to set the VLAN mode for a switch. See **Setting the Switch's VLAN Mode** on page 328.

1. From the Home page, select **Configuration**.

The Configuration System Web Page is displayed. See Figure 82 on page 248.

2. From the Configuration menu, select **Layer 2**.

The MAC Address Web Page is displayed. See Figure 121 on page 330.

3. From the Layer 2 window, select the **VLAN** tab.

The VLAN Web Page is shown in Figure 117.

AT-8400

Configuration

System Name: Middle School Switch
MAC Addr: 00:30:84:EE:31:08

Home System Layer 1 Layer 2 Help Logout

MAC Address **VLAN** Spanning Tree Enhanced Stacking

Total VLANs: 2. Page 1 of 1

	VLAN ID	VLAN Name	Tagged Ports	Untagged Ports	Mgmt
<input checked="" type="radio"/>	1	Default_VLAN	1.4-6	1.1-3,7-8,4.1-8	Yes
<input type="radio"/>	2	Administration	1.5-6		No

Refresh Modify Remove Add

Figure 117 VLAN Web Page

4. Click **Add**.

The Add New VLAN Web Page is displayed in Figure 118.

Add New VLAN

VID : 2

Name : Administration

AT-8411 AT-8411 AT-8411 AT-8411 AT-8411 AT-8411 AT-8401 AT-8411 AT-8411 AT-8411 AT-8411 AT-8411

Port untagged in VLAN
Port tagged in VLAN

Apply Cancel

Figure 118 Add New VLAN Web Page

5. Select the **Name** field and enter a name for the new VLAN.

The name can be from one to 18 characters in length. The name should reflect the function of the nodes of the VLAN (for example, Sales or Accounting). The name can contain spaces but not special characters, such as asterisks (*) or exclamation points (!).

If the VLAN will be unique in your network, the name should be unique as well. However, if the VLAN will be part of a larger VLAN that spans multiple switches, the name for the VLAN needs to be the same on each switch. For example, if VLAN that is called Administration spans three switches, then the VLAN needs to have the same name on all three switches.

Note

You must assign a name to a VLAN.

6. Select the **VID** field and enter a VID value for the new VLAN. The range of the VID value is 2 to 4094. The default is the next available VID number on the switch.

If this will be a unique VLAN in your network, its VID must be unique as well. However, if the VLAN will be part of a larger VLAN that spans multiple switches, assign the same VID value on each switch. For example, if you are creating a VLAN called Sales that will span three switches, you must assign the same VID value to each Sales VLAN on all three switches.

Note

You must assign a VID to a VLAN.

7. To select ports for the VLAN, click on the ports in the switch image.

Clicking repeatedly on a port toggles the port through the following possible settings:



Untagged port



Tagged port



Port not a member of the VLAN

8. Click **Apply**.

The VLAN is created on the switch. The VLAN is now ready for network operations.

Note

The untagged ports that you assign to the new VLAN are automatically removed from their current VLAN assignment.

9. Click **System** from the sidebar.

The Configuration Web Page is displayed.

10. Click **Save Changes** at the bottom of the web page.

The changes you made are saved on the switch.

Modifying a VLAN

To modify a port-based or tagged VLAN, perform the following procedure:

1. From the Home page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. From the Configuration Web Page, select **Layer 2**.
The MAC Dress Web Page is displayed. See Figure 121 on page 330.
3. Select the **VLAN** tab.
The VLAN Web Page is displayed in Figure 117 on page 321.
4. Click the circle next to the name of the VLAN you want to modify.
5. Click **Modify**.
The Modify VLAN Web Page is displayed. See Figure 119.

Modify VLAN

VID : 2

Name : Administration

Legend:
☐ Port untagged in VLAN
☒ Port tagged in VLAN

Buttons: Apply, Cancel

Figure 119 Modify VLAN Web Page

6. Modify the VLAN parameters by referring to Step 5 through Step 7 in the previous procedure, **Creating a VLAN** on page 321.

When modifying a VLAN, observe the following guidelines:

- ☐ You cannot change the VID of a VLAN.
- ☐ You cannot change the name of any VLAN.

7. After making the desired changes, click **Apply**.

The modified VLAN is now ready for network operations.

Note

Untagged ports that are added to a VLAN are automatically removed from their current VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

8. Click **System** from the sidebar.

The Configuration Web Page is displayed.

9. Click **Save Changes** at the bottom of the web page.

The changes you made are saved on the switch.

Deleting VLANs

To delete a port-based or tagged VLAN from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.
The Configuration System Web Page is displayed. See Figure 82 on page 248.
2. From the Configuration Web Page, select **Layer 2**.
The MAC Address Web Page is displayed. See Figure 121 on page 330.
3. From the Layer 2 window, select the **VLAN** tab.
The VLAN Web Page is displayed in Figure 117 on page 321.
4. Click the circle next to the name of the VLAN you want to delete.
5. Click **Remove**.
A confirmation prompt is displayed.
6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.
If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.

Note

You cannot delete the Default_VLAN.

7. Click **System** from the sidebar.
The Configuration Web Page is displayed.
8. Click **Save Changes** at the bottom of the web page.
The changes you made are saved on the switch.

Displaying VLANs

To display all the existing VLANs on a switch, perform the following procedure:

1. Select **Monitoring** from the Home Page.
The Monitoring Web Page is displayed in Figure 83 on page 253.
2. Select **Layer 2** from the sidebar.
3. Select the **VLAN** tab.

The Monitoring VLAN Web Page is shown in Figure 120. The information in this window is for viewing purposes only.

AT-8400

Monitoring

System Name: Middle School Switch
MAC Addr: 00:30:84:EE:31:08

Home
System
Layer 1
Layer 2
Help
Logout

MAC Address VLAN Spanning Tree Port Security Enhanced Stacking

Total VLANs: 2. Page 1 of 1

VLAN ID	VLAN Name	Tagged Ports	Untagged Ports	Mgmt
1	Default_VLAN	1.4-6	1.1-3,7-8,4.1-8	Yes
2	Administration	1.5-6		No

Refresh

Figure 120 Monitoring VLAN Web Page

Setting the Switch's VLAN Mode

This section contains the procedure for setting a switch's VLAN mode. You can configure a switch to support port-based and tagged VLANs or to operate in the Basic VLAN mode. A change to VLAN status is not activated until you reset the switch.

Note

Refer to **Chapter 10, Virtual LANs**, for descriptions of port-based and tagged VLANs and the Basic VLAN mode.

To set the switch's VLAN mode, perform the following procedure:

1. From the Home Page, select **Configuration**.

The Configuration System Web Page is displayed. See Figure 82 on page 248.

2. Scroll down to the Configuration section of the web page. Click either **Tagged** or **Basic** under the Switch Mode heading.

If you select Tagged, which is the default, the switch will support both port-based VLANs and tagged VLANs. If you select Basic, the switch will operate in the Basic VLAN mode.

3. Click **Apply**.

The following confirmation message appears:

The switch will be rebooted for the change to take effect. This page will not be available while the switch reboots. Continue anyway?

4. Select **OK** to continue with the reboot. Select **Cancel** to cancel the reboot.

A change to VLAN status is not activated until you reset the switch.

Chapter 25

MAC Address Table

This chapter describes how to view the dynamic and static addresses in the MAC address table of the switch using a web browser management session. It contains the following procedures:

- ❑ **Viewing the MAC Address Table** on page 330
- ❑ **Adding Static and Multicast MAC Addresses** on page 333
- ❑ **Deleting MAC Addresses** on page 335
- ❑ **Changing the Aging Time** on page 336

Note

For background information on MAC addresses, refer to **MAC Address Overview** on page 201.

Viewing the MAC Address Table

To view the MAC address table, perform the following procedure:

1. From the Home Page, select either **Configuration** or **Monitoring**.

The Configuration System Web Page is displayed in Figure 82 on page 248.

2. Select **Layer 2** from the sidebar.

The MAC Address Web Page is displayed. Figure 121 shows how this window appears when you display it through the Configuration main menu selection.

If you display **MAC Address** tab through the Monitoring main menu selection, the **Add** button is not included. This button is used to add static and multicast addresses to the switch. (For instructions on how to add static and multicast MAC addresses, refer to the next procedure.)

AT-8400

Configuration

System Name: Middle School Switch
MAC Addr: 00:30:84:EE:31:08

Home
System
Layer 1
Layer 2
Help
Logout

MAC Address | VLAN | Spanning Tree | Enhanced Stacking

MAC Addresses Table

☐ View All MAC Addresses
 ☒ View MAC Addresses on Port(s) 1.1-8
 ☐ View Static MAC Addresses
 ☐ View MAC Addresses for VLAN
 ☐ View IP Multicast MAC Addresses
 ☐ View MAC Address

: : : : :

View Add

Figure 121 MAC Addresses Web Page

The options for displaying MAC addresses are described below.

View All MAC Addresses

This option displays both static and dynamic MAC addresses. This is the default setting.

View Static MAC Addresses

This option displays only the static MAC addresses. Static MAC addresses are addresses that you entered manually into the MAC address table.

View IP Multicast Addresses

This option displays the multicast MAC addresses.

View MAC Addresses on Port(s)

This option is used to display the MAC addresses learned on a particular port. For information about how to specify ports, see **Specifying Ports on page 26**.

View MAC Addresses for VLAN

This option displays the MAC addresses learned by a particular VLAN on the switch. You specify the VLAN by its VID.

View MAC Addresses

This option is used to locate the port on the switch where a MAC address was learned or assigned. To use this option, enter the MAC address of the node in the field.

- Once you have selected one of the options, click **View**.

See Figure 122 for an example of the MAC Address Table when you click on the **View MAC addresses on Port(s)**.

	VLAN ID	MAC ADDRESS	PORT	TYPE
<input checked="" type="radio"/>	1	00:00:CD:01:6B:5D	1.1	Dynamic
<input type="radio"/>	1	00:00:CD:01:D3:4B	1.1	Dynamic
<input type="radio"/>	1	00:00:F4:A3:AA:23	1.1	Dynamic
<input type="radio"/>	1	00:00:F4:A4:12:44	1.1	Dynamic
<input type="radio"/>	1	00:00:F4:DD:29:31	1.1	Dynamic
<input type="radio"/>	1	00:01:A5:00:07:8D	1.1	Dynamic
<input type="radio"/>	1	00:02:72:00:22:62	1.1	Dynamic
<input type="radio"/>	1	00:02:DD:30:41:6B	1.1	Dynamic
<input type="radio"/>	1	00:04:5A:65:25:60	1.1	Dynamic
<input type="radio"/>	1	00:06:5B:23:0F:7E	1.1	Dynamic

Total MAC Addresses: 131. Page 1 of 14

Refresh Remove Next Close

Figure 122 MAC Addresses Table Web Page

The MAC addresses are displayed in a table. The columns in the window are defined below:

VLAN ID

The VID of the VLAN to which the port is an untagged member.

MAC ADDRESS

The MAC addresses of the nodes connected to the port.

PORT

The port on the switch where the MAC address was learned or assigned. The port is in the following format: line card number.port number

TYPE

The MAC address type. The type can be either static or dynamic.

4. Click **Close**.

You are returned to the MAC Addresses Table Web Page as shown in Figure 121 on page 330.

Adding Static and Multicast MAC Addresses

This section contains the procedure for assigning static or multicast address to ports on the switch. You can assign up to 255 static MAC addresses per port.

To add a static or multicast address to the MAC address table, perform the following procedure:

1. Select **Configuration** from the Home page.
2. Select **Layer 2** from the sidebar.

The MAC Addresses Web Page is displayed as shown in Figure 121 on page 330.

3. Click **Add**.

The Add Static Unicast MAC Address Web Page is displayed. See Figure 123.

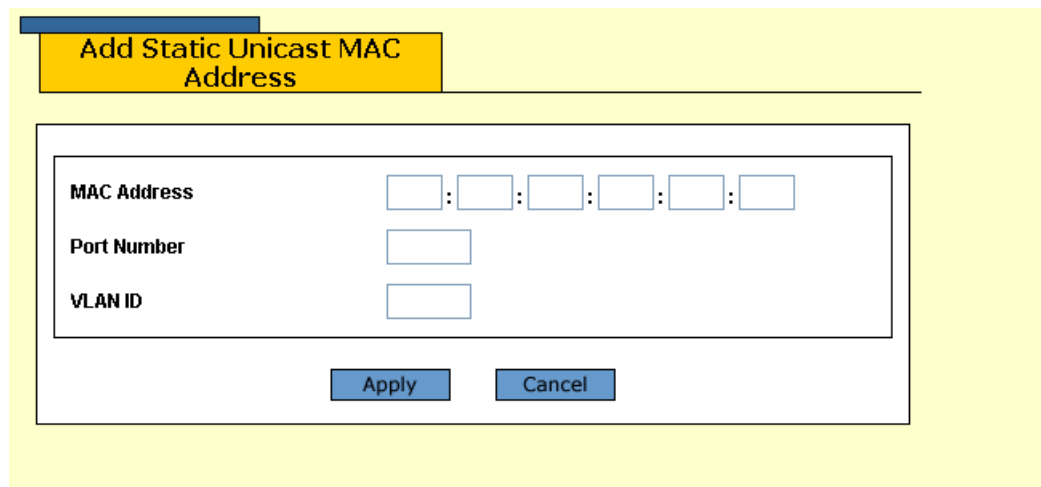


Figure 123 Add Static Unicast MAC Address Web Page

4. In the MAC Address field, enter the new static or multicast MAC address.
5. In the Port Number field, enter the port number that will be assigned the MAC address.

For information about specifying ports, see **Specifying Ports** on page 26.

6. In the VLAN ID field, enter the VLAN ID for the specified port.
The range of VLAN IDs is 1 to 4094, with 1 as the Default_VLAN ID.
7. Click **Apply**.

The MAC Addresses Table is displayed as shown in Figure 121 on page 330.

8. Repeat this procedure to add other static or multicast addresses to the switch.
9. Click **System** from the sidebar.

The Configuration Web Page is displayed.

10. Click **Save Changes** at the bottom of the web page.

The changes you made are saved on the switch.

Deleting MAC Addresses

To delete a static, dynamic, or multicast MAC address from the switch, perform the following procedure:

1. Select **Configuration** from the Home page.
The Configuration System Web Page is displayed Figure 82 on page 248.
2. Select **Layer 2** from the sidebar.
The MAC Addresses Web Page is displayed as shown in Figure 121 on page 330.
3. Display the MAC addresses on the switch by selecting one of the options.
For instructions, refer to **Viewing the MAC Address Table** on page 330.
4. Click **View**.
The MAC Address Table is displayed as shown in Figure 122 on page 331.
5. Click on the dialog circle next to the MAC address that you want to delete from the switch.
6. Click **Remove**.
The address is removed from the MAC address table.
7. Click **Close**.
The MAC Addresses Table Web Page is displayed as shown in Figure 121 on page 330.
8. Click **System** from the sidebar.
The Configuration Web Page is displayed.
9. Click **Save Changes** at the bottom of the web page.
The changes you made are saved on the switch.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of node addresses that are inactive.

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, perform the following procedure:

1. From the Home page, select **Configuration**.
The Configuration System Web Page is displayed Figure 82 on page 248.
2. Scroll down to the bottom of the web page to the Configuration section.
3. Enter a new value, in seconds, in the **MAC Aging Time**.
The range for this field is 8 to 512 seconds.
4. Click **Apply**.
5. Click **Save Changes**.
The changes you made are saved on the switch.

Chapter 26

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. It contains the following procedures:

- ❑ **Configuring IGMP Snooping** on page 338
- ❑ **Displaying a List of Host Nodes and Multicast Routers** on page 341

Note

For background information on this feature, refer to **IGMP Snooping Overview** on page 216.

Configuring IGMP Snooping

To configure IGMP snooping from a web browser management session, perform the following procedure:

1. Select **Configuration** from the Home page.

The Configuration System Web Page is displayed in Figure 82 on page 248.

2. Select the **IGMP** tab.

The Configuration IGMP Web Page is displayed in Figure 124.

The screenshot shows the 'Configuration' web page for a switch. At the top, there's a yellow header with 'Configuration' in large black letters. Below it, a blue bar displays 'System Name: Middle School Switch' and 'MAC Addr: 00:30:84:EE:31:08'. To the right is a small globe icon. On the left, a vertical menu contains buttons for 'Home', 'System', 'Layer 1', 'Layer 2', 'Help', and 'Logout'. The main content area has four tabs: 'General', 'SNMP', 'IGMP' (which is selected), and 'Factory Default'. The 'IGMP' tab is active, showing a configuration box with the following elements:

- A checkbox labeled 'Enable IGMP Snooping' which is currently unchecked.
- A section titled 'Multicast Host Topology' with two radio button options: 'Single-Host/Port (Edge)' (which is selected) and 'Multi-Hosts/Port (Intermediate)'.
- A text input field for 'Host/Router Timeout Interval [1 to 86400]' with the value '260' and the unit 'seconds'.
- A text input field for 'Maximum Multicast Groups [1 to 2048]' with the value '256'.
- An 'Apply' button at the bottom right of the configuration box.

Figure 124 Configuration IGMP Web Page

3. Adjust the IGMP parameters as necessary.

The parameters are explained below:

Enable IGMP Snooping

Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP is enabled.

Multicast Host Topology

Defines whether there is only one host node per port or multiple host nodes per port. Possible settings are Single-Host/Port (Edge) and Multi-Hosts/Port (Intermediate).

Select the Single-Host/Port (Edge) setting when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets from a port under the following conditions:

- ☐ When a host node signals its desire to leave a multicast group by sending a leave request
- ☐ When the host node stops sending reports and times-out

The switch forwards the leave request to the router and simultaneously ceases transmission of multicast packets from the port where the host node is connected.

Select the Multi-Hosts/Port (Intermediate) setting if there is more than one host node connected to a port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected, the switch continues sending multicast packets from a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port continue to receive the multicast packets. Only after all of the host nodes connected to a port have transmitted leave requests (or have timed out) does the switch stop sending multicast packets from the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, select Multi-Hosts/Port (Intermediate).

Host/Router Timeout Interval

Specifies the time period, in seconds, after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

Maximum Multicast Groups

Specifies the maximum number of multicast groups the switch will learn. The range is 1 to 2,048 groups. The default is 256 multicast groups.

This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2,048 addresses. The default is 256 multicast addresses.

4. After setting the IGMP parameters, click **Apply**.
Your changes are activated on the switch.
5. Click **System** from the sidebar.
The Configuration Web Page is displayed.
6. Click **Save Changes** at the bottom of the web page.
The changes you made are saved on the switch.

Displaying a List of Host Nodes and Multicast Routers

You can use the AT-S60 software to display a list of the multicast groups on a switch, as well as the host nodes. In addition, you can view the multicast routers. A multicast router receives multicast packets from a multicast application and transmits the packets to host nodes.

To view host nodes and multicast routers, perform the following procedure:

1. From the Home Page, select **Monitoring**.

The Monitoring Web Page is displayed in Figure 83 on page 253.

2. Select the **IGMP** tab.

The Monitoring IGMP Web Page is displayed in Figure 125.

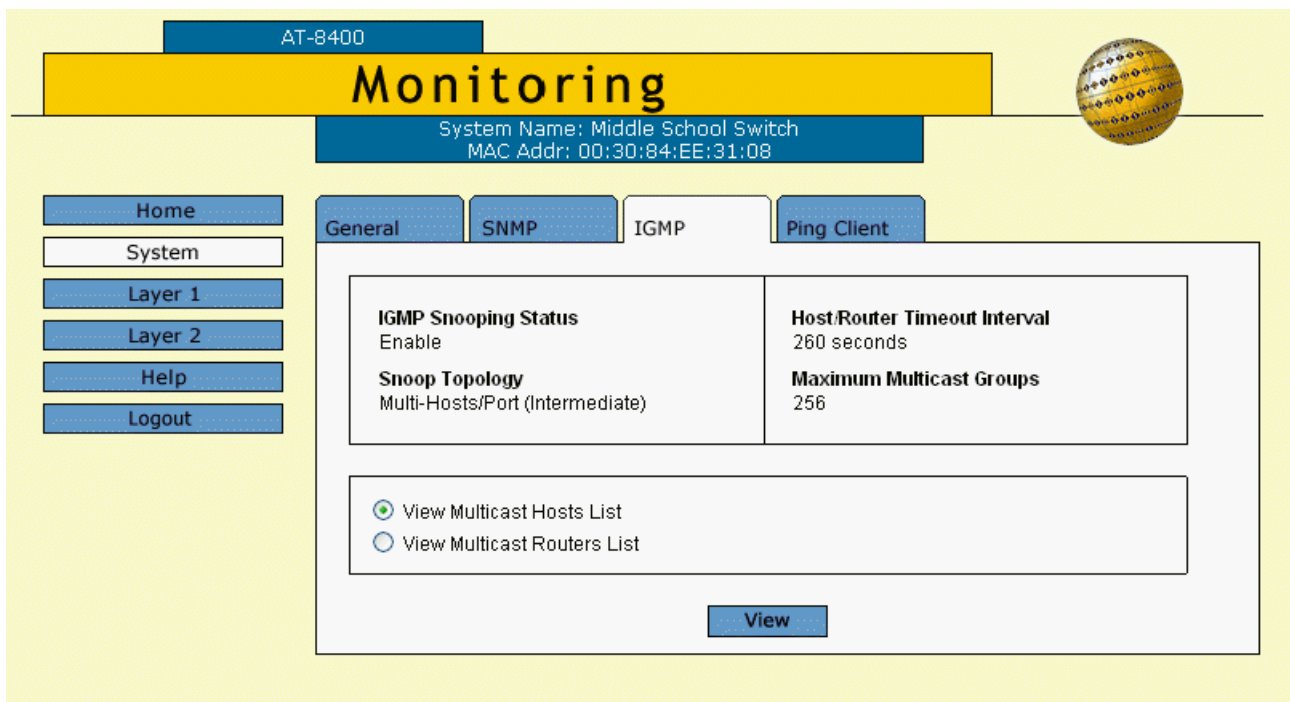


Figure 125 Monitoring IGMP Web Page

3. To view the multicast addresses and the host nodes, click **View Multicast Host List** and then click **View**. To view the multicast routers, click **View Multicast Router List** and then click **View**.

Selecting View Multicast Hosts Lists displays a web page containing the following information. The information in the window is for viewing purposes only.

Multicast Group

The multicast address of the group.

VLAN ID

The VID of the VLAN in which the port is an untagged member.

Member Port

The port(s) on the switch to which one or more host nodes of the multicast group are connected.

Host IP

The IP address(es) of the host node(s) connected to the port.

Status

Indicates IGMP group status of the port.

Active indicates the port is active in the IGMP group.

Left Group indicates the port is not active in the IGMP group.

Selecting View Multicast Routers List displays a web page containing the following information. The information in the window is for viewing purposes only.

Port

The port on the switch where the multicast router is connected.

VLAN ID

The VID of the VLAN in which the port is an untagged member.

Router IP

The IP address of the port on the router.

Appendix A

AT-S60 Default Settings

This appendix lists the AT-S60 factory default settings.

Settings	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
System Name	None
MAC Aging Time	300 seconds
SNMP Communities	
Community Name	public (Read only)
Community Name	private (Read Write)
Spanning Tree Protocol	
Status	Disabled
Bridge Priority	32768
Bridge Max Age Time	20
Bridge Hello Time	2
Bridge Forwarding Delay	15
Port Costs	10 - 10 Mbps 10 - 100 Mbps 4 - 1000 Mbps
Port Priority	128
Fast Mode	No
Rapid Spanning Tree Protocol	
Status	Disabled
Bridge Priority	Increment 8 (32768)
Bridge Max Age Time	20

Settings	Default
Bridge Hello Time	2
Bridge Forwarding Delay	15
Port Costs	Auto detect 2 000 000 - 10 Mbps 200 000 - 100 Mbps 20 000 - 1000 Mbps
Port Priority	Increment 8 (128)
Point-to-Point	Auto Detect
Edge Port	Yes
MSTP	
Status	Disabled
Force Version	MSTP
Bridge Hello Time	2
Bridge Forwarding Delay	15
Bridge Max Age	20
Maximum Hops	20
Configuration Name	null
Revision Level	null
CIST Priority	Increment 8 (32768)
Port Priority	Increment 8 (128)
Port Internal Path Cost	Auto Update
Port External Path Cost	200,000
Point-to-Point	Auto Detect
Edge Port	Yes
IGMP Snooping	
Status	Disabled
Multicast Host Topology	Single Host/ Port (Edge)
Host/Router Time-out Interval	260 seconds
Maximum Multicast Groups	256
Management Interface	
Manager Login Name	manager
Manager Password	friend (case-sensitive)
Operator Login Name	operator
Operator Password	operator (case-sensitive)
Time Out Value	10 minutes

Settings	Default
Twisted Pair Ports	
Status	Enabled
Broadcast Filter	Disabled
Override Priority	No override
HOL Blocking	Disabled
Back Pressure	Disabled
Flow Control	Auto
Negotiation	Auto
Speed	100 Mbps
Security	Automatic
VLANs	
Default VLAN Name	Default_VLAN (all ports)
VID	1
Basic VLAN Mode	Disabled
Broadcast Frame Control	
10/100 Mbps Interval Timer	10 milliseconds
1000 Mbps Interval Timer	100 microseconds
Maximum Number of Frames per Port	0 (disabled)
Management Access	
Telnet	Enabled
SNMP	Disabled
TFTP	Enabled
Web	Disabled
RS-232 Port	
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Data Rate	9600 bps

Index

A

- aging time
 - changing, 211, 336
 - defined, 202
- associations
 - defined, 145
 - VLANs to MSTI IDs, 162
- AT-S39 software updates
 - downloading from a Telnet session, 234
- AT-S60 default settings, 64, 264, 343
- AT-S60 software security, 57
- AT-S60 software updates
 - downloading from a local session, 229
 - obtaining, 228
- AT-S60 version number, 60
- Automatic port security level, 86, 284
- Auto-Negotiation, 83, 273

B

- Basic VLAN mode
 - defined, 184
 - setting, 197, 328
- bootloader version number, 60
- BOOTP
 - activating, 45, 252
 - defined, 45
- BPDU, *see* bridge protocol data unit
- bridge forwarding delay parameter, 131, 137, 158, 302, 306, 311
- bridge hello time parameter, 131, 137, 157, 302, 306, 311
- bridge identifier, 118, 137, 159, 302, 307

- bridge max age parameter, 132, 137, 158, 302, 306, 311
- bridge priority, 118, 131, 136, 159, 302, 306, 312
- bridge protocol data unit (BPDU), 132, 137, 158, 302, 306, 312
- browser tools, 245

C

- CIST priority, 149
- Class of Service
 - configuring, 214
 - defined, 213
- configuration name, 146, 158, 311
- console timeout, 57

D

- default values, AT-S60, 64, 264, 343
- DHCP
 - activating, 45, 252
 - defined, 45
- document conventions, 13
- documentation, 14

E

- enhanced stacking
 - changing switches, 73
 - defined, 32, 36, 68
 - guidelines, 68
 - setting switch status, 71, 266

F

- flow control, 83, 275
- force version, 136, 157, 306, 311
- forwarding delay, 121, 131

G

gateway address, 39, 249, 254

H

hello time, 122, 131

host nodes

defined, 216

displaying, 220, 341

host/router timeout interval, 219, 339

I

IEEE 802.1d standard, 130, 135, 300, 304

IGMP snooping

configuring, 218, 338

defined, 216

Internet Protocol (IP) address, 36, 39, 249, 254

L

limited security mode

defined, 86, 284

local management session

defined, 21

quitting, 32

starting, 29

Lock All Ports security level, 87, 285

M

MAC address table, 200, 330

management access levels, 25, 57

Management Information Base, *see* MIBs

management VLAN, 198

Manager access, 25, 57

Manager password, 57

master switch

assigning, 71, 266

defined, 71, 266

returning to, 75

max hops, 158, 312

MIBs, supported, 24

MSTI priority

defined, 148

MSTP

associations 145

CIST, 145

configuring, 156

connecting VLANs, 153

region, 145

with STP and RSTP, 150

multicast groups, maximum, 219, 339

multicast MAC address

adding, 207, 209, 333

deleting, 335

displaying, 203

multicast router, displaying, 221, 341

Multiple Spanning Tree Protocol

associating VLANs to MSTI IDs, 162

configuring port parameters, 165

creating an MSTI ID, 160

deleting an MSTI ID, 160

O

Operator access, 25, 57

Operator password, 57

P

password

changing, 39, 250

default, 31, 33

pinging, 63, 263

port

configuring parameters, 81, 271

disable, 82, 274

displaying status, 77, 276

speed, 84

statistics, 223

port cost

defined, 120

setting, 133, 139, 303, 307

port mirroring

creating, 109, 293

defined, 108

deleting, 111, 113, 114, 115, 293

port security

configuring, 88

defined, 86

displaying, 283

port trunking

creating, 97, 287

defined, 93

deleting, 99, 100, 287

guidelines, 94

modifying, 290

port VLAN identifier (PVID)

defined, 172, 180

port-based VLAN

creating, 187, 191, 321

defined, 171

deleting, 196, 326

- displaying, 327
- modifying, 193, 324
- priority queues, 213
- priority, 133, 139, 303, 307

Q

- quitting
 - local session, 32
 - Telnet interface, 34
 - web browser session, 245

R

- Rapid Spanning Tree Protocol
 - configuring port parameters, 138
- regional root, 148
- resetting a switch, 56, 262
- revision level, 158, 312
- revision number, 146
- root bridge, 118
- RS-232 port, default settings, 30

S

- Secure level, port security, 87, 284
- slave switch
 - assigning, 71, 266
 - defined, 71, 266
- SNMP community strings, 47, 256
- SNMP management session, 24, 57
- snoop topology, 218, 338
- software updates
 - downloading from a local session, 229
 - downloading from a Telnet session, 234
 - obtaining, 17, 228
- Spanning Tree Protocol
 - configuring bridge parameters, 130, 135, 298
 - configuring port parameters, 132
 - defined, 117
 - port cost, 120, 133, 139, 303, 307
 - viewing bridge parameters, 317
- starting session
 - local, 29
 - Telnet, 33
 - web browser, 243
- static MAC address
 - adding, 207, 209, 333
 - deleting, 335
 - displaying, 203
- statistics
 - port, 223

- STP. See Spanning Tree Protocol
- subnet mask, 39, 249, 254
- system name, 39, 249

T

- tagged VLAN
 - creating, 187, 192, 321
 - defined, 179
 - deleting, 196, 326
 - displaying, 327
 - modifying, 193, 324
- Telnet management interface
 - quitting, 34
- Telnet management session
 - defined, 22
 - starting, 33
- TFTP, downloading and uploading files, 229, 234

U

- unavailable status, defined, 71, 266
- user name, default, 31, 33

V

- version number, AT-S60, 60
- virtual LAN
 - creating, 187, 191, 192, 321
 - defined, 169
 - deleting, 196, 326
 - displaying, 327
 - mode, changing, 197, 328
 - modifying, 193, 324
 - port-based, defined, 171
 - tagged, defined, 179
- VLAN identifier (VID), 171, 189
- VLAN identifier, 322
- VLAN. See virtual LAN

W

- web browser management session
 - defined, 23
 - disabling, 57
 - limitations, 23
 - quitting, 245
 - starting, 243